

Benutzerhandbuch



Warenzeichen und Copyright

Warenzeichen

Windows ist ein registriertes Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und anderen Ländern.
Alle anderen Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Eigentümer.
Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

Hinweise zum Copyright

Für Avira Antivirus Suite wurde Code von Drittanbietern verwendet. Wir bedanken uns bei den Copyright-Inhabern dafür, dass sie uns ihren Code zur Verfügung gestellt haben.
Detaillierte Informationen zum Copyright finden Sie unter "Third Party Licenses" in der Programmhilfe von Avira Antivirus Suite.

Endbenutzer-Lizenzvereinbarung - EULA

http://www.avira.com/de/license-agreement

Privatsphäre

http://www.avira.com/de/general-privacy



Inhaltsverzeichnis











1. Einleitung

Mit Ihrem Avira Produkt schützen Sie Ihren Computer vor Viren, Würmern, Trojanern, Ad- und Spyware sowie weiteren Gefahren. Verkürzend wird in diesem Handbuch von Viren oder Malware (Schadsoftware) und unerwünschten Programmen gesprochen.

Das Handbuch beschreibt die Installation und Bedienung des Programms.

Auf unserer Webseite können Sie vielfältige Optionen und weitere Informationsmöglichkeiten nutzen:

http://www.avira.de

Sie können auf der Avira Webseite:

- Informationen zu weiteren Avira Desktop-Programmen abrufen
- die aktuellsten Avira Desktop-Programme herunterladen
- die aktuellsten Produkthandbücher im Format PDF herunterladen
- kostenfreie Support- und Reparatur-Werkzeuge herunterladen
- die umfassenden Wissensdatenbank und FAQ-Artikel bei der Behebung von Problemen nutzen
- die landesspezifischen Supportadressen abrufen.

Ihr Avira Team

1.1 Symbole und Hervorhebungen

Folgende Symbole werden verwendet:

Symbol / Bezeichnung	Erläuterung
✓	Steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss.
▶	Steht vor einem Handlungsschritt, den Sie ausführen.
↳	Steht vor einem Ergebnis, das aus der vorangehenden Handlung folgt.
Warnung	Steht vor einer Warnung bei Gefahr von kritischem Datenverlust.

Hinweis	Steht vor einem Hinweis mit besonders wichtigen Informationen oder vor einem Tipp, der das Verständnis und die Nutzung Ihres Avira Produkts erleichtert.

Folgende Hervorhebungen werden verwendet:

Hervorhebung	Erläuterung
Kursiv	Dateiname oder Pfadangabe.
	Elemente der Software-Oberfläche, die angezeigt werden (z.B. Fensterbereich oder Fehlermeldung).
Fett	Elemente der Software-Oberfläche, die angeklickt werden (z.B. Menüpunkt, Rubrik, Optionsfeld oder Schaltfläche).



2. Produktinformationen

In diesem Kapitel erhalten Sie alle Informationen, die für den Erwerb und Einsatz Ihres Avira Produkts relevant sind:

- siehe Kapitel: Leistungsumfang
- siehe Kapitel: Systemvoraussetzungen
- siehe Kapitel: Lizenzierung und Upgrade
- siehe Kapitel: Lizenzverwaltung

Avira Produkte bieten umfassende und flexible Werkzeuge, um Ihren Computer zuverlässig vor Viren, Malware, unerwünschten Programmen und sonstigen Gefahren zu schützen.

- Beachten Sie:

Warnung
Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch das beste Virenschutzprogramm kann Sie nicht hundertprozentig vor Datenverlust schützen. Fertigen Sie regelmäßig Sicherungskopien (Backups) Ihrer Daten an.

Hinweis
Ein Programm, das vor Viren, Malware, unerwünschten Programmen und sonstigen Gefahren schützt, ist nur dann zuverlässig und wirksam, wenn es aktuell ist. Stellen Sie die Aktualität Ihres Avira Produkts über automatische Updates sicher. Konfigurieren Sie das Programm entsprechend.

2.1 Leistungsumfang

Ihr Avira Produkt verfügt über folgende Funktionen:

- Control Center zur Überwachung, Administration und Steuerung des gesamten Programms
- Zentrale Konfiguration mit benutzerfreundlicher Standard- und Expertenkonfiguration und kontextsensitiver Hilfe
- System-Scanner (On-Demand Scan) mit profilgesteuerter und konfigurierbarer Suche nach allen bekannten Typen von Viren und Malware
- Integration in die Windows Benutzerkontensteuerung (User Account Control), um Aufgaben durchführen zu können, für die administrative Rechte erforderlich sind.
- Echtzeit-Scanner (On-Access Scan) zur ständigen Überwachung sämtlicher Dateizugriffe



- ProActiv-Komponente zur permanenten Überwachung von Programmaktionen (nur für 32-Bit-Systeme)
- Email-Schutz (POP3-Scanner, IMAP-Scanner und SMTP-Scanner) zur permanenten Kontrolle Ihrer Emails auf Viren und Malware, inklusive Überprüfung der Email-Anhänge
- Avira SearchFree Toolbar, eine im Webbrowser integrierte Suchleiste, mit der Sie schnell und bequem das Internet durchsuchen können. Sie beinhaltet auch Widgets zu den wichtigsten Funktionen rund ums Internet.
- Browser-Schutz zur Überwachung der aus dem Internet per HTTP-Protokoll übertragenen Daten und Dateien (Überwachung der Ports 80, 8080, 3128)
- Avira Kinderschutz für Soziale Netzwerke informiert Eltern über die Onlineaktivitäten ihrer Kinder. Das System prüft die Konten der sozialen Netzwerke auf Kommentare, Fotos usw., die dem Ruf ihres Kindes schaden könnten oder die darauf hinweisen könnten, dass Ihr Kind gefährdet ist.
- Avira Free Android Security ist eine App nicht nur mit Antidiebstahlmaßnahmen. Die App bietet Funktionen, mit deren Hilfe Sie das mobile Gerät ausfindig machen können, wenn Sie es verlegt haben oder schlimmer noch: wenn es gestohlen wurde. Des Weiteren ermöglicht Ihnen die App, eingehende Anrufe und SMS zu blockieren. Avira Free Android Security schützt Mobiltelefone und Smartphones, die mit dem Betriebssystem Android arbeiten.
- Integriertes Quarantäne-Management zur Isolation und Behandlung verdächtiger Dateien
- Rootkits-Schutz zum Auffinden von Malware, die versteckt im System des Rechners installiert wurde (sog. Rootkits)
  (nicht verfügbar unter Windows XP 64 Bit)
- Direkter Zugriff auf detaillierte Informationen zu gefundenen Viren und Malware über das Internet
- Einfaches und schnelles Update des Programms, der Virendefinitionsdateien (VDF) sowie der Suchengine durch Single File Update und inkrementelles VDF-Update über einen Webserver im Internet
- Benutzerfreundliche Lizenzierung in der Lizenzverwaltung
- Integrierter Planer zur Festsetzung von einmaligen oder wiederkehrenden Aufgaben wie Updates oder Prüfläufen
- Extrem hohe Viren- und Malware-Erkennung durch innovative Suchtechnologien (Suchengine) inklusive heuristischer Suchverfahren
- Erkennung aller gebräuchlichen Archivtypen inklusive Erkennung verschachtelter Archive und Smart-Extension-Erkennung
- Hohe Performanz durch Multithreading-Fähigkeit (gleichzeitiges Scannen vieler Dateien mit hoher Geschwindigkeit)

2.2 Systemvoraussetzungen

2.2.1 Systemanforderungen Avira Antivirus Suite

Avira Antivirus Suite stellt für einen erfolgreichen Einsatz folgende Anforderungen an das System:

Betriebssystem

- Windows 8, neuestes SP (32 oder 64 Bit) oder
- Windows 7, neuestes SP (32 oder 64 Bit) oder
- Windows XP, neuestes SP (32 oder 64 Bit)

Hardware

- Computer ab Pentium, mindestens 1 GHz
- Mindestens 150 MB freier Speicherplatz auf der Festplatte (bei Verwendung der Quarantäne und für temporären Speicher mehr)
- Mindestens 1024 MB Arbeitsspeicher unter Windows 8, Windows 7,
- Mindestens 512 MB Arbeitsspeicher unter Windows XP

Weitere Voraussetzungen

- Für die Programminstallation: Administrator-Rechte
- Für alle Installationen: Windows Internet Explorer 6.0 oder höher
- Ggf. Internetverbindung (siehe Installation vorbereiten)

2.2.2 Systemanforderungen Avira SearchFree Toolbar

Folgende Voraussetzungen sind für eine reibungslose Nutzung der Avira SearchFree Toolbar erforderlich:

Betriebssystem

- Windows 8, neuestes SP (32 oder 64 Bit) oder
- Windows 7, neuestes SP (32 oder 64 Bit) oder
- Windows XP, neuestes SP (32 oder 64 Bit)

Webbrowser

- Windows Internet Explorer 6.0 oder höher
- Mozilla Firefox 3.0 oder höher
- Google Chrome 18.0 oder höher

Hinweis
Bitte deinstallieren Sie ggf. bereits installierte Suchleisten bevor Sie die Avira SearchFree Toolbar installieren. Anderenfalls ist eine Installation der Avira SearchFree Toolbar nicht möglich.

2.2.3 Hinweise für die Benutzer von Windows Vista oder höher

Unter Windows XP arbeiten viele Benutzer mit Administratorrechten. Dies ist unter Sicherheitsaspekten jedoch nicht wünschenswert, denn so haben auch Viren und unerwünschte Programme leichtes Spiel, sich im Computer einzunisten.

Aus diesem Grund führte Microsoft die "Benutzerkontensteuerung" (User Account Control) ein. Diese ist Teil folgender Betriebssysteme:

- Windows Vista
- Windows 7
- Windows 8

Die Benutzerkontensteuerung bietet mehr Schutz für Anwender, die als Administrator angemeldet sind. So verfügt ein Administrator zunächst nur über die Privilegien eines normalen Benutzers. Aktionen, für die Administratorrechte erforderlich sind, markiert das Betriebssystem klar mit einem Hinweissymbol. Zudem muss der Anwender die gewünschte Aktion explizit bestätigen. Erst, nachdem diese Zustimmung eingeholt ist, findet eine Erhöhung der Privilegien statt, und das Betriebssystem führt die jeweilige administrative Aufgabe aus.

Avira Antivirus Suite benötigt für einige Aktionen Administratorrechte. Diese Aktionen werden mit folgendem Zeichen gekennzeichnet: . Erscheint dieses Zeichen zusätzlich auf einer Schaltfläche, so werden zum Ausführen dieser Aktion Administratorrechte benötigt. Besitzt Ihr aktuelles Benutzerkonto keine Administratorrechte, so fordert Sie der Windows-Dialog zur Benutzerkontensteuerung zur Eingabe des Administratorpassworts auf. Verfügen Sie über kein Administratorpasswort, so können Sie diese Aktion nicht ausführen.

2.2.4 Inkompatibilitäten mit anderen Programmen

Avira Antivirus Suite

Avira Antivirus Suite kann derzeit nicht mit folgenden Produkten betrieben werden:

- PGP Desktop Home
- PGP Desktop Professional 9.0
- CyberPatrol

Ein Fehlverhalten in den genannten Produkten kann dazu führen, dass der Avira Email-Schutz (POP3 -Scanner) der Avira Antivirus Suite nicht arbeitet oder das System instabil wird. Avira arbeitet zusammen mit PGP und CyberPatrol an einer Lösung des Problems. Bis dahin empfehlen wir dringend, die genannten Produkte vor der Installation von Avira Antivirus Suite zu deinstallieren.

Avira Browser-Schutz

Avira Browser-Schutz ist mit folgenden Produkten nicht kompatibel:

- Teleport Pro von Tennyson Maxwell, Inc
- CHIPDRIVE® Time Recording von SCM Microsystems
- MSN Messenger von Microsoft

Daher werden gesendete und angeforderte Daten dieser Produkte vom Avira Browser-Schutz ignoriert.

> **Note**
> Der Avira Email-Schutz ist nicht funktionsfähig, wenn auf demselben Computer bereits ein Mailserver (bspw. AVM KEN, Exchange, ...) installiert ist.

2.3 Lizenzierung und Upgrade

2.3.1 Lizenzierung

Um Ihr Avira Produkt nutzen zu können, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen an.

Die Lizenz wird in Form eines Aktivierungscodes vergeben. Der Aktivierungscode ist ein Buchstaben-Zahlen-Code, den Sie beim Erwerb des Avira Produkts erhalten. Über den Aktivierungscode sind die genauen Daten Ihrer Lizenz, d.h. welche Programme für welchen Zeitraum lizenziert wurden, erfasst.

Der Aktivierungscode wird Ihnen in einer Email übermittelt, falls Sie Ihr Avira Produkt im Internet erworben haben, oder ist auf der Produktverpackung vermerkt.

Um Ihr Programm zu lizenzieren, geben Sie den Aktivierungscode bei der Aktivierung des Programms ein. Die Produktaktivierung kann bei der Installation erfolgen. Sie können Ihr Avira Produkt jedoch auch nach der Installation im Lizenzmanager unter **Hilfe > Lizenzmanagement** aktivieren.

2.3.2 Lizenzverlängerung

Wenn Ihre Lizenz in Kürze abläuft, erinnert Sie Avira durch ein Slide-Up, sie zu verlängern. Um dies zu tun, müssen Sie nur einen Link klicken und Sie werden zum Avira

Online-Shop weitergeleitet. Es ist aber auch möglich, die Lizenz Ihres Avira Produkts durch den Lizenzmanager zu verlängern, unter **Hilfe > Lizenzmanagement**.

Wenn Sie sich im Lizenzportal von Avira registriert haben, können Sie Ihre Lizenz auch zusätzlich durch die **Lizenzübersicht** verlängern oder die automatische Verlängerung wählen.

2.3.3 Upgrade

Im Lizenzmanager haben Sie die Möglichkeit, ein Upgrade auf ein Produkt aus der Avira Desktop-Produktfamilie anzustoßen: Eine manuelle Deinstallation des alten Produkts und eine manuelle Installation des neuen Produkts sind dadurch nicht erforderlich. Beim Upgrade aus dem Lizenzmanager geben Sie den Aktivierungscode des Produkts, auf das Sie umsteigen möchten, im Eingabefeld des Lizenzmanagers an. Es erfolgt eine automatische Installation des neuen Produkts.

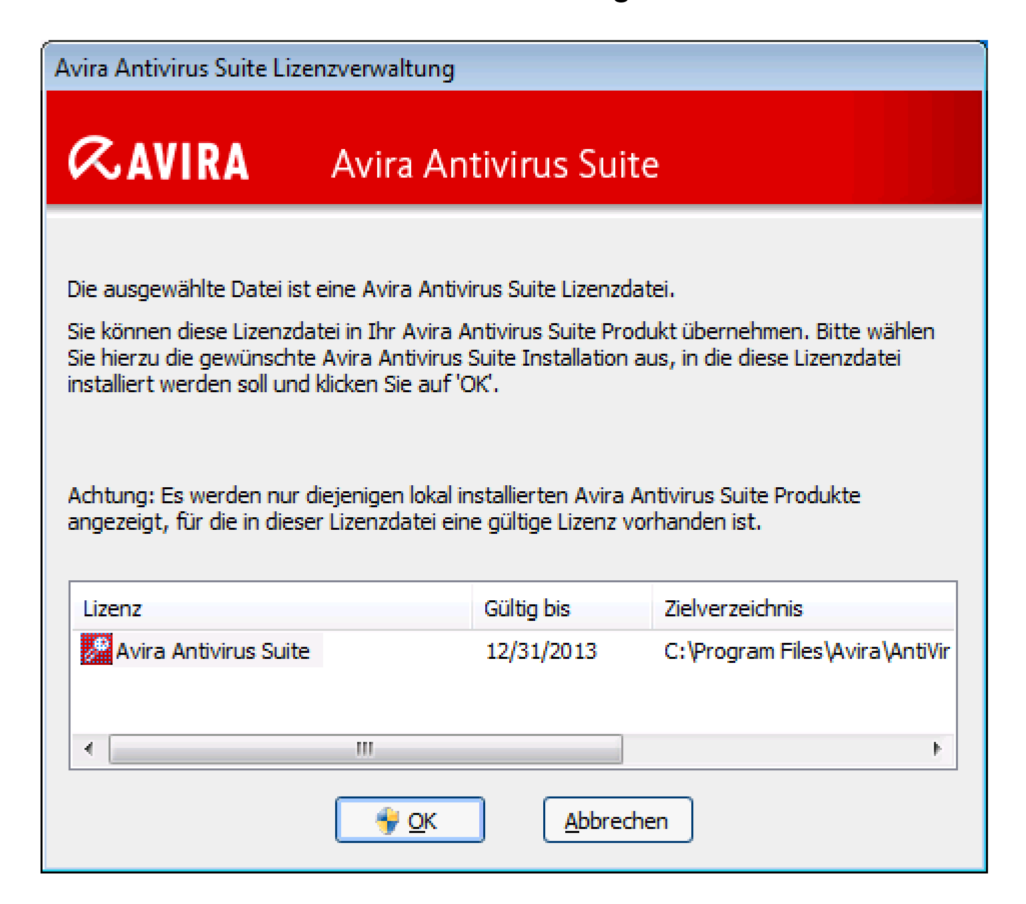
Um hohe Zuverlässigkeit und Sicherheit für Ihren Computer zu erreichen, erinnert Sie Avira an das anstehende Upgrade auf die neueste Version. Klicken Sie auf **Upgrade** in dem Popup-Element, um auf die produktspezifische Upgrade-Seite Ihres Produkts weitergeleitet zu werden. Sie haben die Möglichkeit, für Ihr derzeitiges Produkt ein Upgrade durchzuführen oder ein umfangreicheres Avira Produkt zu erwerben. Die Übersichtsseite der Avira Produkte zeigt Ihnen, welches Produkt Sie gegenwärtig verwenden und gibt Ihnen die Möglichkeit, dieses mit anderen Avira Produkten zu vergleichen. Für weitere Informationen klicken Sie das Informations-Symbol rechts neben dem Produktnamen an. Wenn Sie bei Ihrem bisherigen Produkt bleiben möchten, klicken Sie **Upgrade**, um sofort die neueste Version mit verbesserten Funktionen zu installieren. Wenn Sie ein umfangreicheres Produkt erwerben möchten, klicken Sie **Kaufen** am unteren Ende der entsprechenden Produktspalte. Sie werden dann in den Avira Online-Shop weitergeleitet, um Ihre Bestellung durchzuführen.

> **Hinweis**
> In Abhängigkeit von Ihrem Produkt und Ihrem Betriebssystem benötigen Sie eventuell Administratorrechte, um das Upgrade durchzuführen. Melden Sie sich als Administrator an, bevor Sie ein Upgrade ausführen.

2.3.4 Lizenzverwaltung

Die Avira Antivirus Suite Lizenzverwaltung ermöglicht eine sehr einfache Installation der Avira Antivirus Suite Lizenz.

Avira Antivirus Suite Lizenzverwaltung



Sie können eine Installation der Lizenz vornehmen, in dem Sie in ihrem Dateimanager oder der Aktivierungs-Email mit Doppelklick die Lizenzdatei auswählen und den entsprechenden Bildschirmanweisungen folgen.

> **Hinweis**
> Die Avira Antivirus Suite Lizenzverwaltung kopiert die entsprechende Lizenz automatisch in den entsprechenden Produktordner. Ist bereits eine Lizenz vorhanden, erscheint ein Hinweis, ob die bestehende Lizenzdatei ersetzt werden soll. Die bereits bestehende Datei wird in diesem Fall mit der aktuellen Lizenzdatei überschrieben.



3. Installation und Deinstallation

In diesem Kapitel finden Sie Informationen rund um die Installation von Avira Antivirus Suite.

- Installation vorbereiten
- Von CD installieren während Sie offline sind
- Heruntergeladene Software installieren
- Inkompatible Software entfernen
- Eine Installationsart wählen
- Avira Antivirus Suite installieren
- Die Installation ändern
- Avira Antivirus Suite deinstallieren

3.1 Installation vorbereiten

- ✓ Überprüfen Sie vor der Installation, ob Ihr Computer die Systemvoraussetzungen erfüllt.
- ✓ Schließen Sie alle laufenden Anwendungen.
- ✓ Vergewissern Sie sich, dass keine weiteren Virenschutzlösungen installiert sind. Die automatischen Schutzfunktionen verschiedener Sicherheitslösungen können sich gegenseitig behindern (automatische Optionen siehe Entfernen inkompatibler Software).
- ✓ Bitte deinstallieren Sie ggf. bereits installierte Suchleisten bevor Sie die Avira SearchFree Toolbar installieren. Anderenfalls ist eine Installation der Avira SearchFree Toolbar nicht möglich.
- ✓ Stellen Sie eine Internetverbindung her.

- Die Verbindung wird zur Ausführung folgender Installationsschritte benötigt:
  - Herunterladen der aktuellen Programmdateien und der Suchengine sowie der tagesaktuellen Virendefinitionsdateien durch das Installationsprogramm (bei internetbasierter Installation)
  - Aktivierung des Programms
  - Registrierung als Benutzer
  - Ggf. Ausführung eines Updates nach beendeter Installation

- ✓ Halten Sie den Aktivierungscode oder die Lizenzdatei für Avira Antivirus Suite bereit, wenn Sie das Programm aktivieren möchten..
- ✓ Zur Produktaktivierung oder Registrierung kommuniziert Avira Antivirus Suite über das HTTP-Protokoll und Port 80 (Web-Kommunikation) sowie über das Verschlüsselungsprotokoll SSL und Port 443 mit den Avira Servern. Falls Sie eine Firewall nutzen, stellen Sie sicher, dass die benötigten Verbindungen und eingehende oder ausgehende Daten nicht von der Firewall blockiert werden.

3.2 Von CD installieren während Sie offline sind

- Legen Sie die Avira Antivirus Suite CD ein.

  Wenn die Funktion Autostart aktiviert ist, klicken Sie auf **Ordner öffnen**, um alle Dateien anzuzeigen.
  ODER

  Navigieren Sie zu Ihrem CD-Laufwerk, klicken Sie mit der rechten Maustaste auf AVIRA und wählen Sie **Ordner öffnen**, um alle Dateien anzuzeigen.

  Doppelklicken Sie auf die Datei *autorun.exe*.

  Wählen Sie im CD-Menü die Offline-Version zur Installation.

  Das Programm prüft, ob inkompatible Software vorhanden ist (nähere Informationen hier: Entfernen inkompatibler Software).

  Die Installationsdatei wird entpackt. Die Installationsroutine wird gestartet.

  Fahren Sie fort mit Eine Installationsart wählen.

3.3 Von der Avira Webseite heruntergeladene Software installieren

- Öffnen Sie die Seite www.avira.com/download.

  Wählen Sie ein Produkt und klicken Sie **Download starten**.

  Speichern Sie die heruntergeladene Datei auf Ihrem System.

  Doppelklicken Sie die Installationsdatei avira_antivirus_suite_de.exe.

  Klicken Sie **Ja**, wenn das Dialogfeld Benutzerkontensteuerung angezeigt wird.

  Das Programm prüft, ob inkompatible Software vorhanden ist (nähere Informationen hier: Entfernen inkompatibler Software).

  Die Installationsdatei wird entpackt. Die Installationsroutine wird gestartet.

  Fahren Sie fort mit Eine Installationsart auswählen.

> **Hinweis**
> Wenn nötig, können Sie die Installation jederzeit abbrechen und zu einem späteren Zeitpunkt fortsetzen. Eine Verknüpfung wird auf Ihrem Desktop erstellt. Um die Installation fortzusetzen, doppelklicken Sie die mit dem Avira Logo versehene Verknüpfung *Installation fortsetzen*.

3.4 Inkompatible Software entfernen

Avira Antivirus Suite wird Ihren Computer auf mögliche inkompatible Software durchsuchen. Bei Fund inkompatibler Software generiert Avira Antivirus Suite eine entsprechende Liste dieser Programme. Es wird empfohlen, Software, die die Sicherheit Ihres Computers gefährdet, zu deinstallieren.

- Wählen Sie aus der Liste jene Programme, die automatisch von Ihrem Computer entfernt werden sollen und klicken Sie **Weiter**.

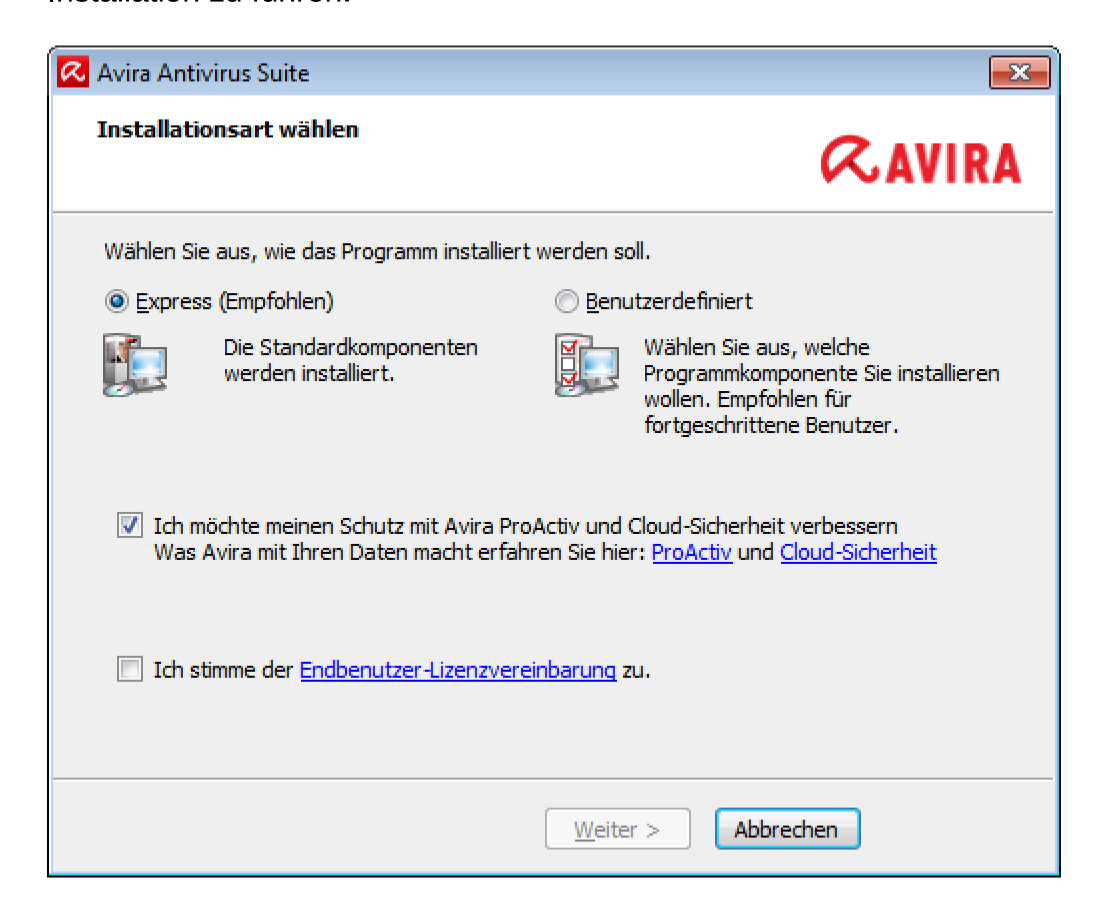
  Für einige Produkte muss die Deinstallation manuell bestätigt werden.

  Wählen Sie diese Programme aus und klicken Sie **Weiter**.

  Die Deinstallation eines oder mehrerer Programme kann den Neustart Ihres Computers erfordern. Nach dem Neustart beginnt die Installation.

3.5 Eine Installationsart wählen

Während der Installation können Sie im Installationsassistenten einen Setup-Typ auswählen. Der Installationsassistent ist dafür ausgelegt, Sie reibungslos durch die Installation zu führen.



Verwandte Themen:

- Eine Expressinstallation durchführen
- Eine benutzerdefinierte Installation durchführen

3.5.1 Eine Expressinstallation durchführen

Die *Expressinstallation* ist die empfohlene Setup-Routine.

- Sie installiert alle Standardkomponenten der Avira Antivirus Suite. Es werden die von Avira empfohlenen Einstellungen für das Sicherheitsniveau verwendet.



- Standardmäßig wird einer der folgenden Installationspfade gewählt:
  - *C:\Programme\Avira* (für Windows 32-Bit-Versionen) oder
  - *C:\Programme (x86)\Avira* (für Windows 64-Bit-Versionen)
- Hier finden Sie alle Dateien der Avira Antivirus Suite.
- Wenn Sie diese Installationsart gewählt haben, können Sie die Installation bequem durch **Weiter** klicken zum Abschluss bringen.
- Diese Installationsart ist für Anwender konzipiert, die mit der Konfiguration von Software-Tools nicht hinreichend vertraut sind.

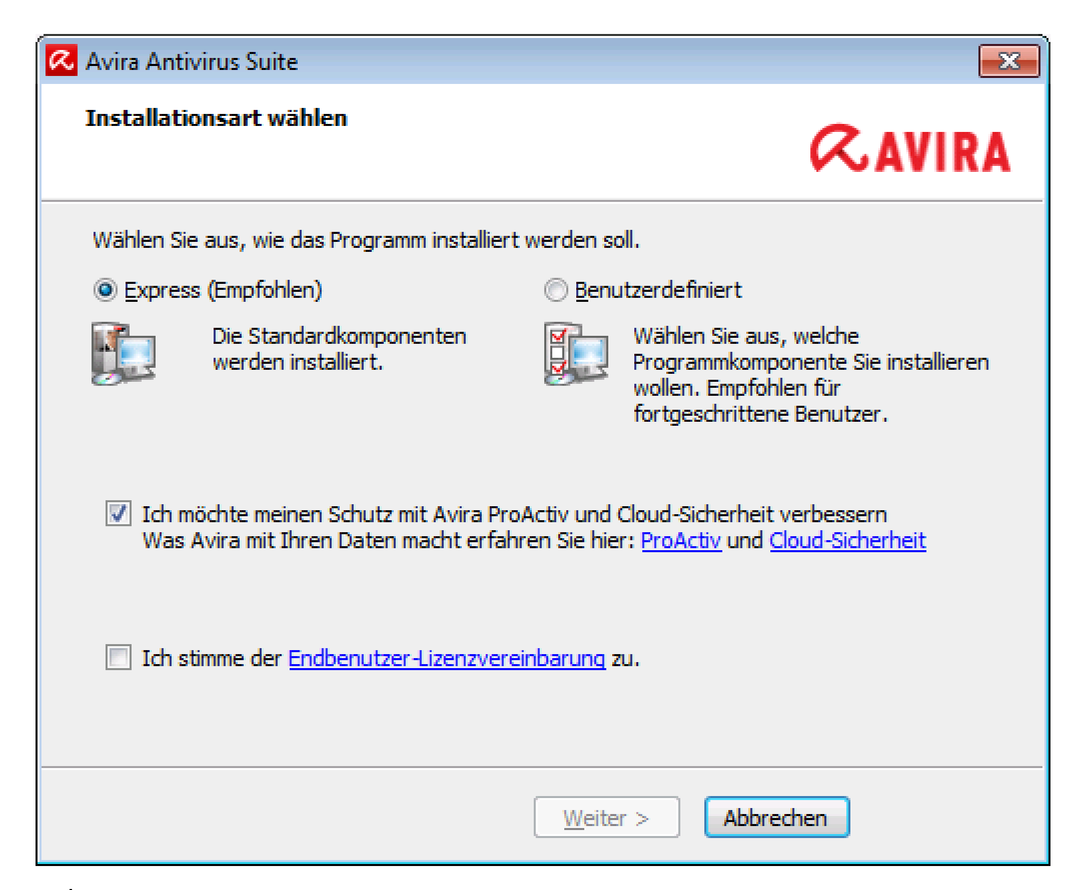
3.5.2 Eine benutzerdefinierte Installation durchführen

Die *Benutzerdefinierte Installation* ermöglicht es, Ihre Installation zu konfigurieren. Dies empfiehlt sich für fortgeschrittene Anwender, die mit Hard- und Software sowie sicherheitsrelevanten Fragen bestens vertraut sind.

- Sie haben die Möglichkeit, einzelne Programmkomponenten zur Installation zu wählen.
- Es kann ein Zielordner für die zu installierenden Programmdateien gewählt werden.
- Sie können das **Erstellen eines Desktopsymbols und einer Programmgruppe im Startmenü** deaktivieren.
- Mithilfe des Konfigurationsassistenten können Sie benutzerdefinierte Einstellungen für Avira Antivirus Suite festlegen. Darüber hinaus können Sie Ihr persönliches Sicherheitsniveau wählen.
- Nach der Installation können Sie eine kurze, automatische Systemprüfung veranlassen.



3.6 Avira Antivirus Suite installieren



- Wenn Sie nicht an der Avira Community teilnehmen möchten, deaktivieren Sie das standardmäßig aktivierte Kontrollkästchen **Ich möchte meinen Schutz mit Avira ProActiv und Cloud-Sicherheit verbessern**.

  Wenn Sie Ihre Teilnahme an der Avira Community bestätigen, sendet Avira Antivirus Suite Daten über verdächtige Programme an das Avira Malware Research Center. Die Daten werden ausschließlich zu einer erweiterten Onlineprüfung und zur Erweiterung und Optimierung der Erkennung genutzt.

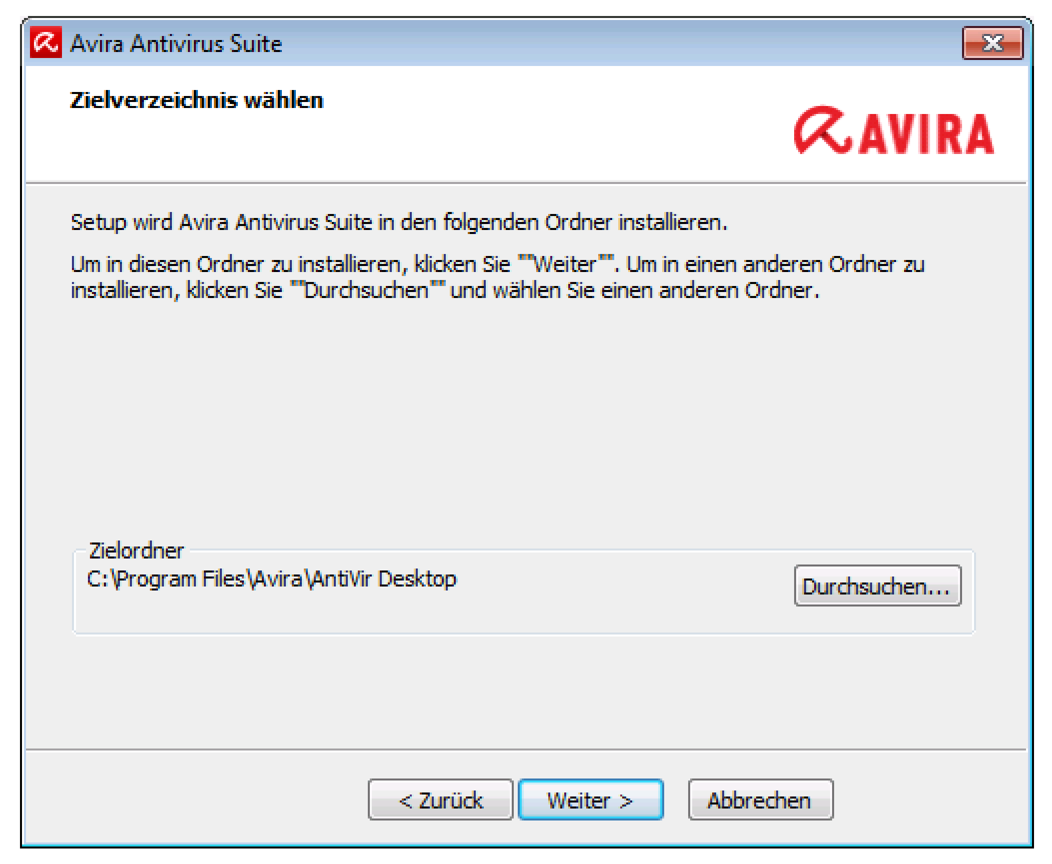
  Über die Links **ProActiv** und **Cloud-Sicherheit** können Sie Details zur erweiterten Online- und Cloud-Prüfung abrufen.

  Bestätigen Sie, dass Sie die **Endbenutzer-Lizenzvereinbarung** akzeptieren. Wenn Sie die Details der **Endbenutzer-Lizenzvereinbarung** einsehen möchten, klicken Sie auf den Link.

3.6.1 Einen Zielordner wählen

Die benutzerdefinierte Installation erlaubt Ihnen einen Ordner zu wählen, um Avira Antivirus Suite zu installieren.





- Klicken Sie **Durchsuchen** und navigieren Sie zu dem Ort, wo Sie Avira Antivirus Suite installieren möchten.

  Im Fenster **Zielverzeichnis wählen** wählen Sie den Ordner aus, wo Sie Avira Antivirus Suite installieren möchten.

  Klicken Sie **Weiter**.

3.6.2 Avira SearchFree Toolbar installieren

Am Ende des Setups können Sie die Avira SearchFree Toolbar installieren.

Avira SearchFree Toolbar beinhaltet zwei Hauptkomponenten: Avira SearchFree und die schon bekannte Toolbar.

Mithilfe von Avira SearchFree können Sie das Internet nach beliebigen Begriffen durchsuchen. Bewertet mit einer Sicherheitseinstufung, zeigt die Suchengine alle Treffer im Browserfenster an. Sie ermöglicht Avira-Benutzern eine umfangreiche und sichere Suche.

Die Toolbar bietet Ihnen drei Anwendungen zu den wichtigsten Funktionen rund ums Internet. Mit nur einem Klick haben Sie direkten Zugriff auf Facebook und zu Ihren Emails, oder können die sichere Internetsuche aktivieren (nur Firefox und Internet Explorer).





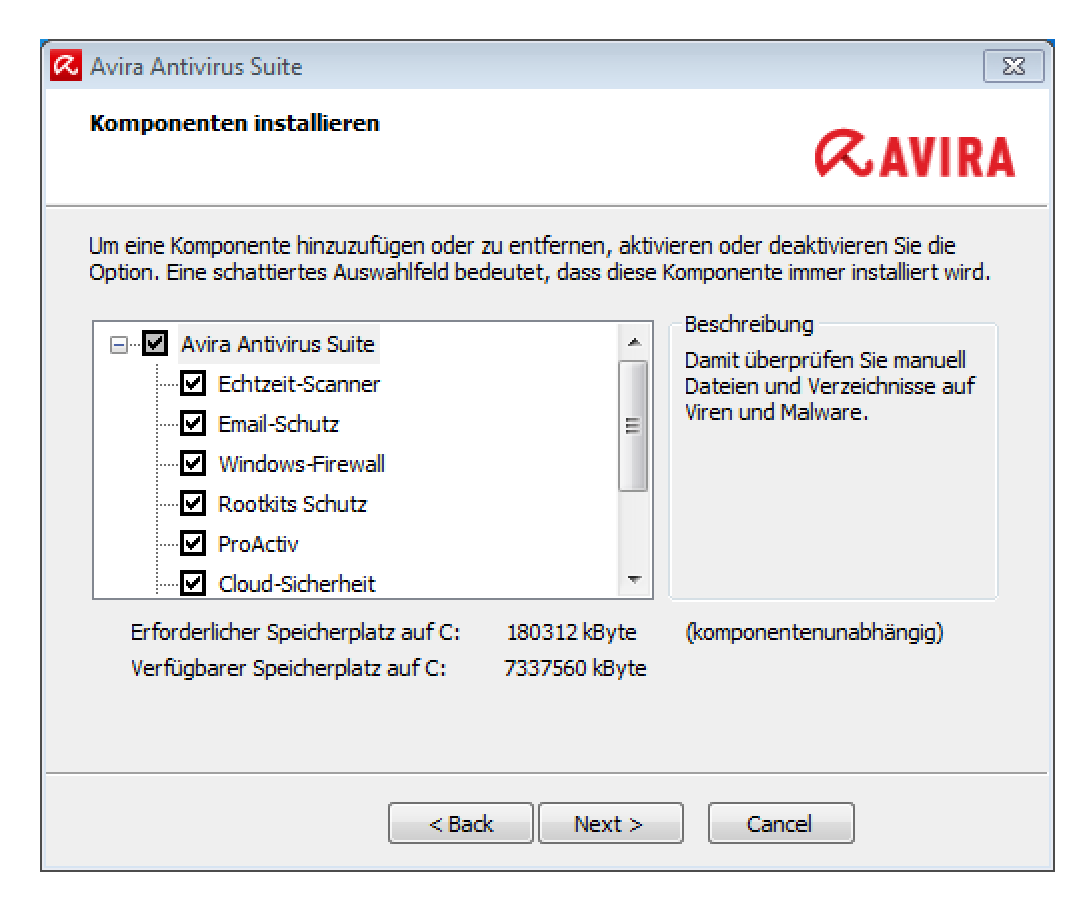
- Wenn Sie die Avira SearchFree Toolbar nicht installieren möchten, entfernen Sie die Markierung aus dem Dialogfeld **Avira SearchFree (avira.search.ask.com) als Startseite und für neue Tabs im Browser einstellen und beibehalten.**

  Wenn Sie ablehnen, wird nur das Setup der Avira SearchFree Toolbar abgebrochen. Die Installation von Avira Antivirus Suite wird dennoch abgeschlossen.

3.6.3 Komponenten für die Installation wählen

Bei einer benutzerdefinierten Installation oder einer Änderungsinstallation können folgende Komponenten zur Installation ausgewählt, hinzugefügt oder entfernt werden.





Aktivieren oder deaktivieren Sie die Komponenten im Dialogfeld Komponenten installieren.

- **Avira Antivirus Suite**
  Dies beinhaltet alle Komponenten, die für eine erfolgreiche Installation von Avira Antivirus Suite benötigt werden.
  - **Echtzeit-Scanner**
    Der Avira Echtzeit-Scanner läuft im Hintergrund. Er überwacht und repariert ggf. Dateien bei Operationen wie Öffnen, Schreiben und Kopieren in Echtzeit. Im Echtzeit-Modus prüft Avira Antivirus Suite die Datei automatisch bei jedem Dateivorgang (Laden, Ausführen, Kopieren). Beim Dateivorgang Umbenennen wird kein Scan durch den Avira Echtzeit-Scanner ausgelöst.
  - **Email-Schutz**
    Email-Schutz ist die Schnittstelle zwischen Ihrem Computer und dem Email-Server, von dem Ihr Email-Programm (Email-Client) die Emails herunterlädt. Email-Schutz hängt sich als sogenannter Proxy zwischen das Email-Programm und den Email-Server. Alle eingehenden Emails werden durch diesen Proxy geleitet, dabei auf Viren bzw. unerwünschte Programme geprüft und an Ihr Email-Programm weitergeleitet. Je nach Konfiguration verarbeitet das Programm die betroffenen Emails automatisch oder fragt Sie nach einer bestimmten Aktion.
  - **Windows Firewall** (ab Windows 7)
    Diese Komponente steuert die Windows Firewall durch Avira Antivirus Suite.
  - **Rootkit-Schutz**
    Avira Rootkit-Schutz prüft, ob auf Ihrem Computer bereits Software installiert wurde, die nach dem Eindringen in das Computersystem mit den herkömmlichen Methoden der Malware-Erkennung nicht gefunden werden kann.

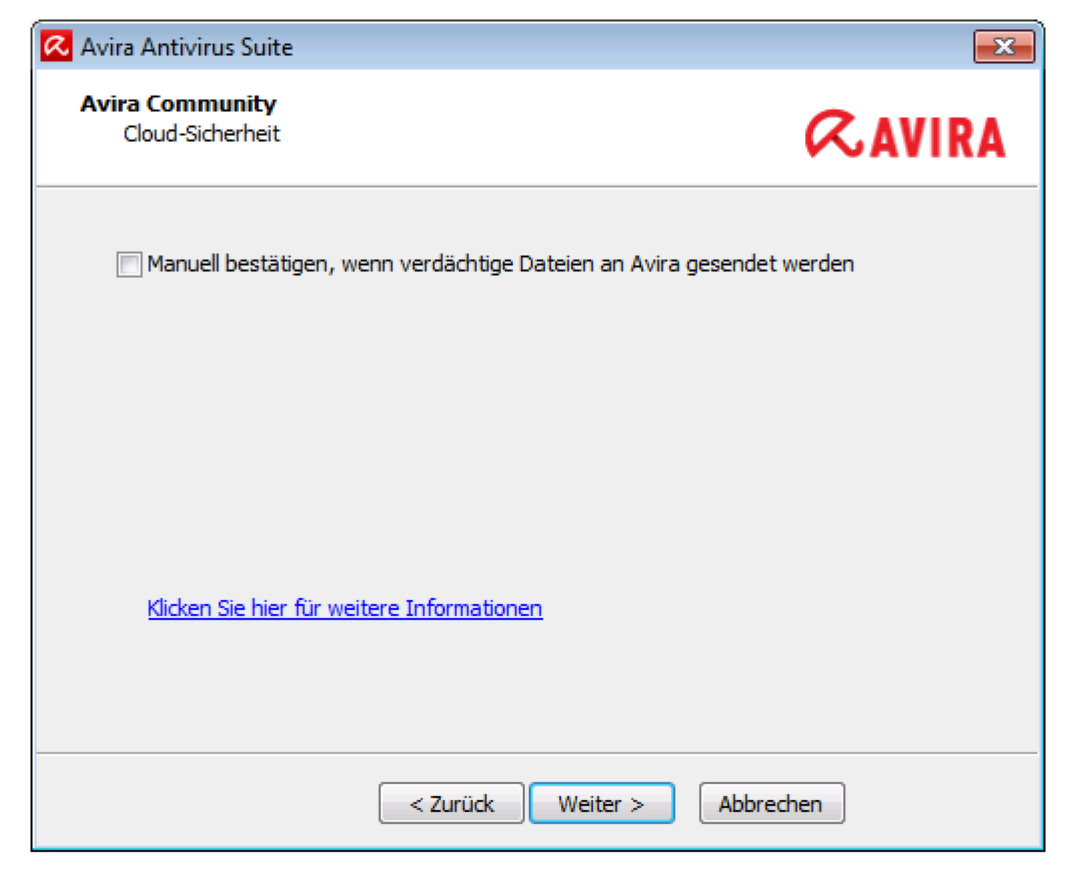


- **ProActiv**
  Die ProActiv-Komponente überwacht Aktionen von Anwendungen und meldet ein verdächtiges Verhalten von Anwendungen. Mit dieser verhaltensbasierten Erkennung können Sie sich vor unbekannter Malware schützen. Die ProActiv-Komponente ist in den Avira Echtzeit-Scanner integriert.
- **Cloud-Sicherheit**
  Die Cloud-Sicherheit-Komponente ist ein Modul zur dynamischen Online-Erkennung bisher unbekannter Malware. Das heißt, dass die Dateien in Echtzeit zu einem Remotestandort hochgeladen und dort mit bekannten Dateien und anderen, hochgeladenen Dateien verglichen und analysiert werden (nicht geplant und ohne Verzögerung). Auf diese Weise wird die Datenbank beständig aktualisiert, demzufolge ein noch höheres Maß an Sicherheit geboten werden kann.
  Wenn Sie die Cloud-Sicherheit-Komponente ausgewählt haben, Sie jedoch jedesmal manuell bestätigen möchten, welche Dateien zur Cloud-Analyse hochgeladen werden sollen, aktivieren Sie die Option **Manuell bestätigen, wenn verdächtige Dateien an Avira gesendet werden**.
- **Browser-Schutz**
  Bei der Internetnutzung fordern Sie über Ihren Webbrowser Daten von einem Webserver an. Die vom Webserver übertragenen Daten (HTML-Dateien, Skript- und Bilddateien, Flash-Dateien, Video- und Musik-Streams usw.) gelangen normalerweise vom Browser-Cache direkt zur Ausführung in den Webbrowser, sodass eine Prüfung durch eine Echtzeitsuche, wie bei Avira Echtzeit-Scanner, nicht möglich ist. Auf diesem Weg können Viren und unerwünschte Programme in Ihr Computersystem gelangen. Der Browser-Schutz ist ein sogenannter HTTP-Proxy, der die zur Datenübertragung genutzten Ports (80, 8080, 3128) überwacht und die übertragenen Daten auf Viren und unerwünschte Programme prüft. Je nach Konfiguration verarbeitet das Programm die betroffenen Dateien automatisch oder lässt den Benutzer eine bestimmte Aktion auswählen.
- **Shellerweiterung**
  Die Shellerweiterung erzeugt im Kontextmenü des Windows Explorers (rechte Maustaste) den Eintrag **Ausgewählte Dateien mit Avira überprüfen**. Mit diesem Eintrag können Sie einzelne Dateien oder Verzeichnisse direkt scannen.

Verwandte Themen:
Installation ändern

Wenn Sie sich für eine Teilnahme an der Avira Community entschieden haben, können Sie wählen, ob Sie den Upload verdächtiger Dateien zum Avira Malware Research Center jedesmal manuell bestätigen möchten.

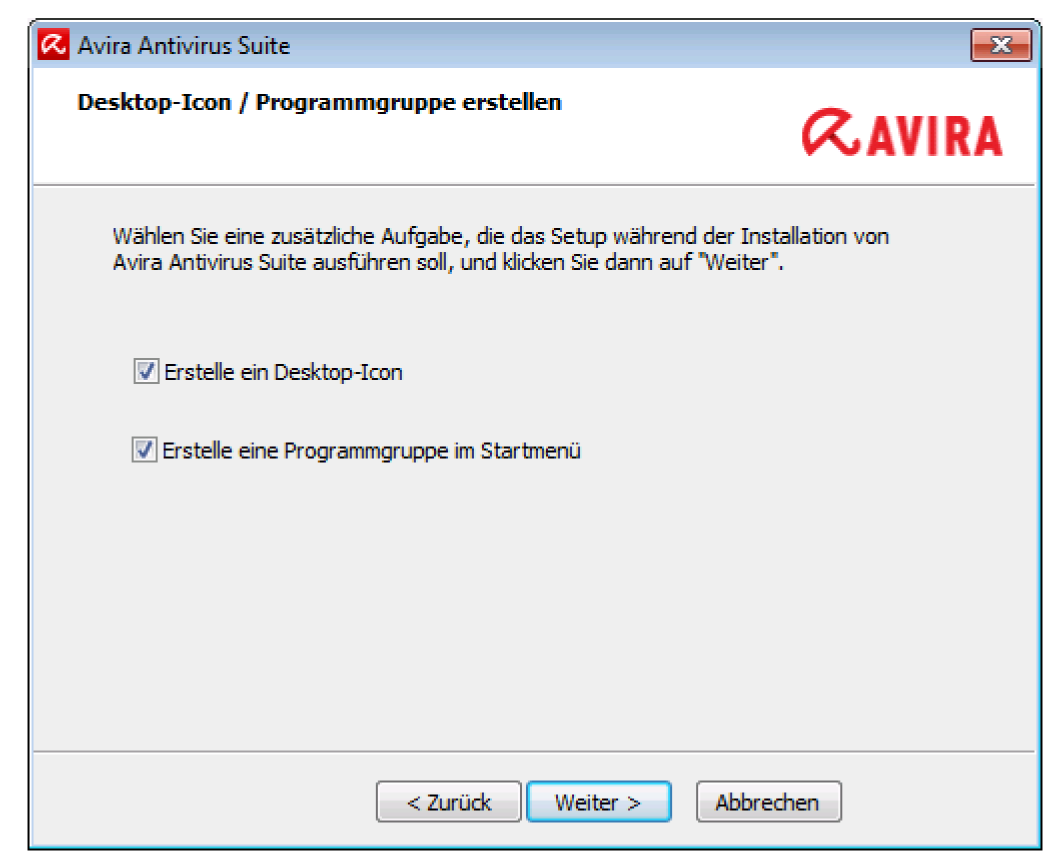




- Damit Avira Antivirus Suite jedesmal eine Bestätigung von Ihnen fordert, aktivieren Sie die Option**Manuell bestätigen, wenn verdächtige Dateien an Avira gesendet werden**.

3.6.4 Verknüpfungen für Avira Antivirus Suite erstellen

Das Erstellen eines Desktopsymbols und/oder einer Programmgruppe im Startmenü hilft Ihnen, einfacher und schneller auf Avira Antivirus Suite zuzugreifen.



- Um eine Desktop-Verknüpfung für Avira Antivirus Suite und/oder eine Programmgruppe im **Startmenü** zu erstellen, lassen Sie die Option(en) aktiviert.

3.6.5 Avira Antivirus Suite aktivieren

Es gibt mehrere Wege, Avira Antivirus Suite zu aktivieren.





Wenn Sie bereits einen Aktivierungscode erhalten haben, geben Sie diesen in die vorgesehenen Felder ein.

- Wenn Sie noch einen Aktivierungscode benötigen, klicken Sie auf den Link zum Erwerben eines Aktivierungscodes.

  Sie werden auf die Avira Webseite weitergeleitet, wo Sie einen Aktivierungscode erwerben können.

- Wenn Sie das Produkt zunächst testen wollen, wählen Sie **Produkt testen** aus und geben Sie Ihre Daten in die erforderlichen Felder der Registrierung ein.

  Ihre Evaluationslizenz hat eine Gültigkeit von 31 Tagen.

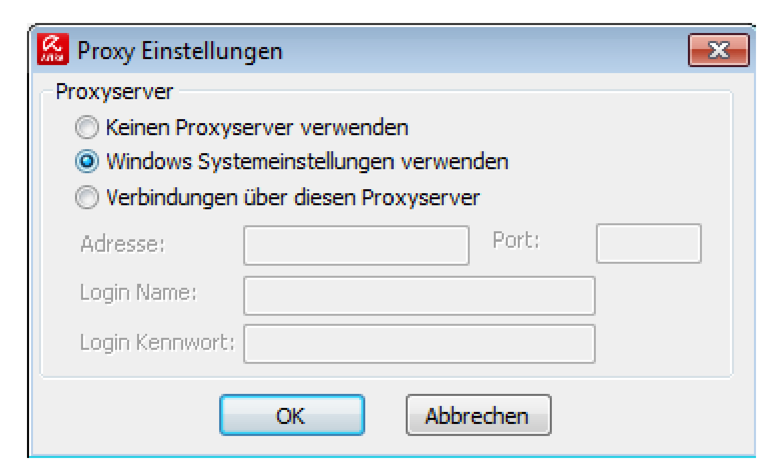
- Wenn Sie bereits ein Produkt aktiviert haben und Ihr Avira Produkt erneut installieren möchten, wählen Sie die Option **Ich habe bereits eine gültige Lizenzdatei** aus.

  Ein Browserfenster öffnet sich und Sie können in Ihrem System zu der Datei *hbedv.key* navigieren.

3.6.6 Proxyeinstellungen definieren

Das Festlegen der Proxyeinstellungen empfiehlt sich für fortgeschrittene Anwender, die bestens vertraut sind mit Hard- und Software sowie sicherheitsrelevanten Fragen.





- Wenn Avira Antivirus Suite sich nicht über einen Proxyserver mit dem Internet verbinden soll, aktivieren Sie die Option **Keinen Proxyserver verwenden**.
- Wenn Sie möchten, dass sich Avira Antivirus Suite auf die gleiche Weise mit dem Internet verbindet wie alle anderen installierten Anwendungen, lassen Sie die Option **Windows Systemeinstellungen verwenden** (standardmäßig aktiviert) aktiviert.

  Sie können die Windows Systemeinstellungen zur Verwendung eines Proxyservers unter **Systemsteuerung > Internetoptionen > Verbindungen > LAN-Einstellungen** konfigurieren. Im Internet Explorer können Sie im Menü **Extras** ebenfalls auf die Internetoptionen zugreifen.

> **Hinweis**
> Wenn Sie einen Proxyserver verwenden, der eine Authentifizierung erfordert, geben Sie alle erforderlichen Daten unter der Option **Verbindungen über diesen Proxyserver** ein. Die Option **Windows Systemeinstellungen verwenden** kann nur für Proxyserver ohne Authentifizierung genutzt werden.

- Um einen Proxyserver einzurichten, der vornehmlich Avira Antivirus Suite zur Verfügung stehen soll, aktivieren Sie **Verbindungen über diesen Proxyserver** und geben Sie alle relevanten Informationen ein:

Adresse

Geben Sie den Rechnernamen oder die IP-Adresse des Proxyservers ein, den Sie für die Verbindung mit dem Webserver verwenden möchten.

Beispiele:

Adresse: proxy.domain.com

Adresse: 192.168.1.100

Port

Geben Sie die Port-Nummer des Proxyservers ein, den Sie für die Verbindung mit dem Webserver nutzen möchten.

Beispiele:



Port: 8080

Port: 3128

Benutzername

Geben Sie einen Benutzernamen für die Anmeldung am Proxyserver ein.

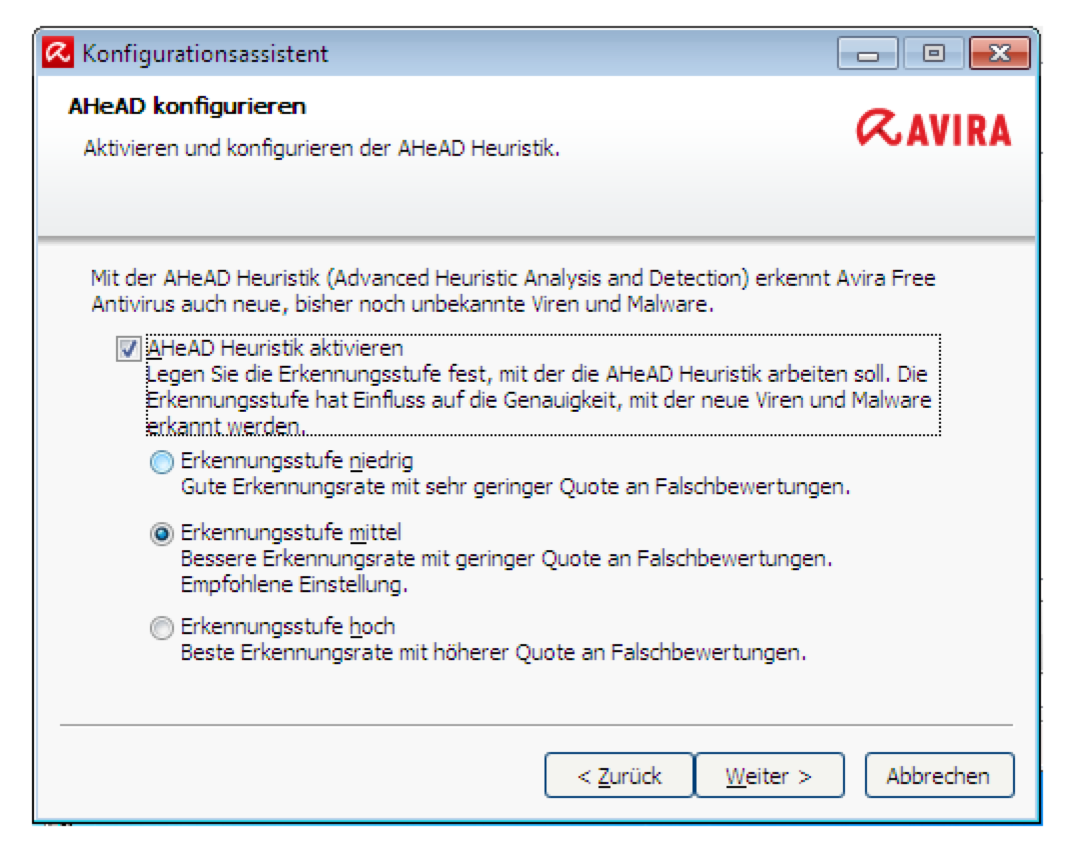
Anmeldungspasswort

Geben Sie das entsprechende Passwort für die Anmeldung am Proxyserver ein. Das Passwort wird verschlüsselt gespeichert. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

Klicken Sie auf **OK**.

3.6.7 Heuristische Erkennungsstufe (AHeAD) konfigurieren

Avira Antivirus Suite beinhaltet mit der Avira AHeAD-Technologie (*Advanced Heuristic Analysis and Detection*) ein sehr leistungsfähiges Tool. Diese Technologie verwendet Erkennungsmustertechniken, sodass unbekannte (neue) Malware durch vorausgegangene Analyse anderer Malware erkannt werden kann.



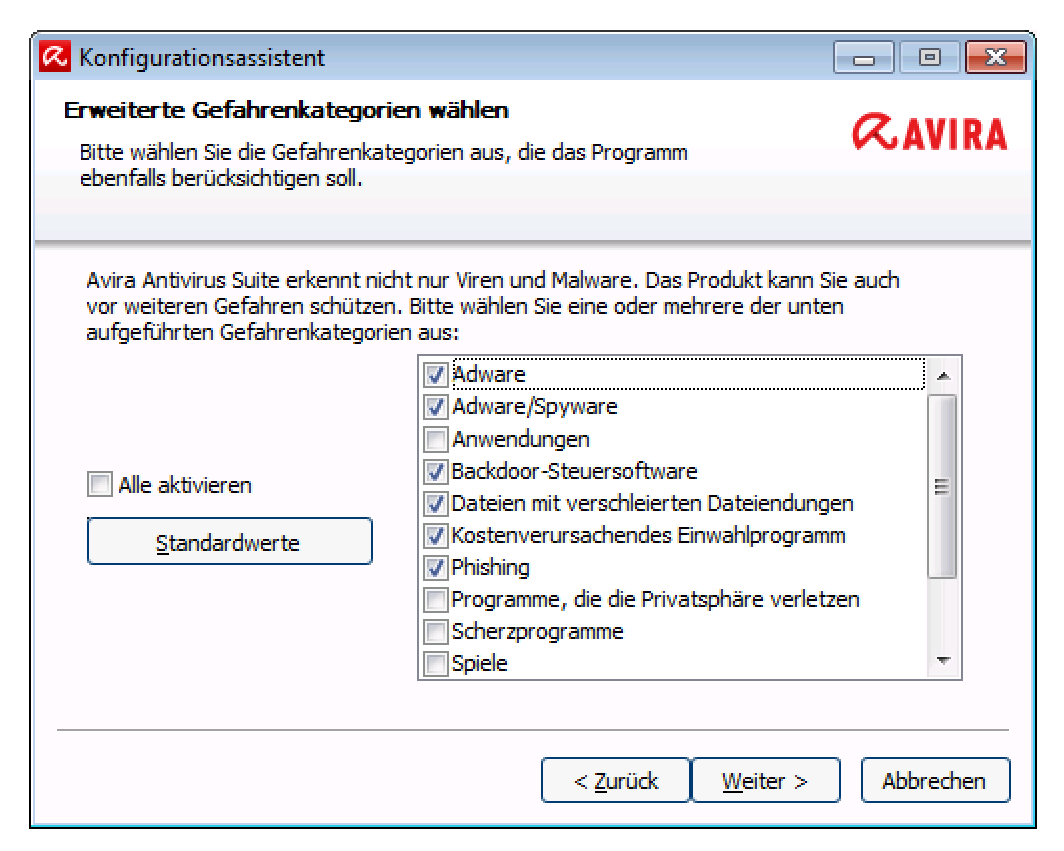
- Wählen Sie im Dialogfenster **AHeAD konfigurieren** eine Erkennungsstufe aus und klicken Sie **Weiter**.

Die gewählte Erkennungsstufe wird für die Einstellung der AHeAD-Technologie des System-Scanners (Direktsuche) und des Echtzeit-Scanners (Echtzeitsuche) übernommen.



3.6.8 Erweiterte Gefahrenkategorien auswählen

Viren und Malware sind nicht die einzigen Gefahren, die ein Risiko für Ihren Computer darstellen. Wir haben eine ganze Liste an Risiken definiert und diese für Sie als Erweiterte Gefahrenkategorien geordnet.



- Eine Anzahl von Gefahrenkategorien ist bereits standardmäßig vorausgewählt.

  Aktivieren Sie ggf. weitere Gefahrenkategorien im Dialogfenster **Erweiterte Gefahrenkategorien wählen**.

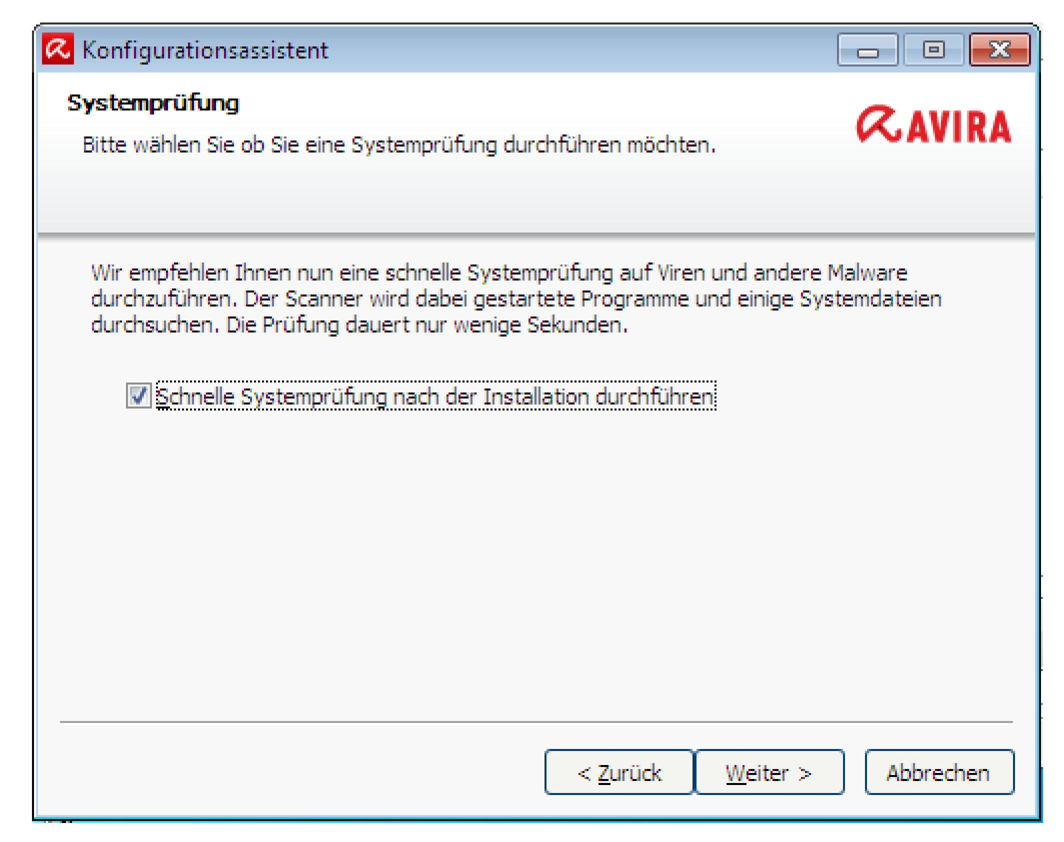
  Wenn Sie Ihre Meinung ändern, können sie zu den empfohlenen Werten zurückkehren, indem Sie die Schaltfläche **Standardwerte** klicken.

  Um mit der Installation fortzufahren, klicken Sie **Weiter**.

3.6.9 Einen Scan nach der Installation starten

Um den aktuellen Sicherheitsstatus Ihres Computers zu prüfen, kann nach abgeschlossener Konfiguration und vor dem Neustart des Computers eine schnelle Systemprüfung durchgeführt werden. Der System-Scanner prüft gestartete Programme und die wichtigsten Systemdateien auf Viren und Malware.





- Wenn Sie eine schnelle Systemprüfung durchführen möchten, lassen Sie die Option **Schnelle Systemprüfung** aktiviert.

  Klicken Sie **Weiter**.

  Klicken Sie **Fertig stellen**, um die Konfiguration zu beenden.

  Wenn Sie die Option **Schnelle Systemprüfung** nicht deaktiviert haben, führt der System-Scanner eine schnelle Systemprüfung durch.

3.7 Die Installation ändern

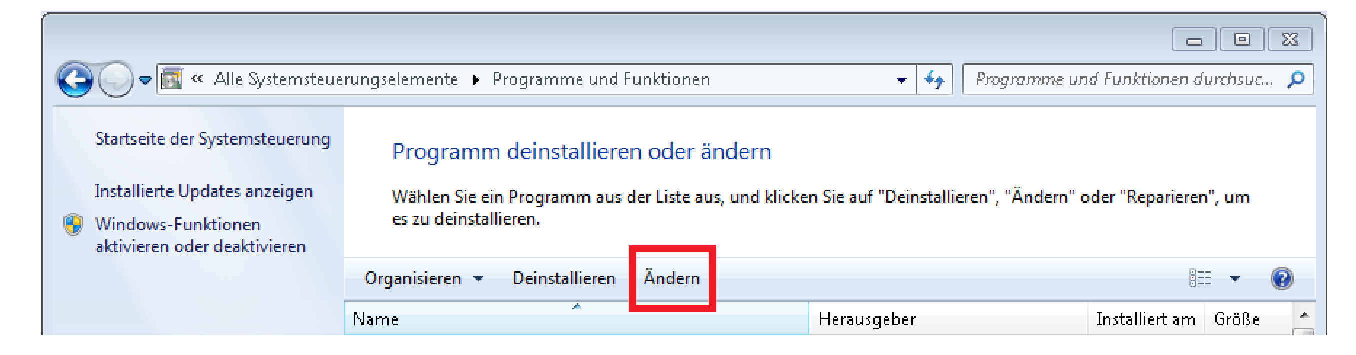
Wenn Sie Ihrer gegenwärtigen Installation Module hinzufügen oder Module entfernen möchten, können Sie dies tun, ohne Avira Antivirus Suite zu deinstallieren. So funktioniert es:

- Installation unter Windows 8 ändern
- Installation unter Windows 7 ändern
- Installation unter Windows XP ändern

3.7.1 Installation unter Windows 8 ändern

Sie haben die Möglichkeit, einzelne Programmkomponenten der aktuellen Avira Antivirus Suite Installation hinzuzufügen oder zu entfernen (siehe Komponenten für die Installation wählen).





Wenn Sie Programmkomponenten der aktuellen Installation hinzufügen oder entfernen möchten, können Sie in der **Windows-Systemsteuerung** die Option **Programm deinstallieren** zum **Ändern/Deinstallieren** von Programmen verwenden.

- Klicken Sie mit der rechten Maustaste auf den Bildschirm.

  Das Symbol **Alle Apps** erscheint.

  Klicken Sie auf das Symbol und suchen Sie unter *Apps - System* nach **Systemsteuerung**.

  Doppelklicken Sie auf das Symbol **Systemsteuerung**.

  Klicken Sie auf **Programme - Programm deinstallieren**.

  Klicken Sie auf **Programme und Features - Programm deinstallieren**.

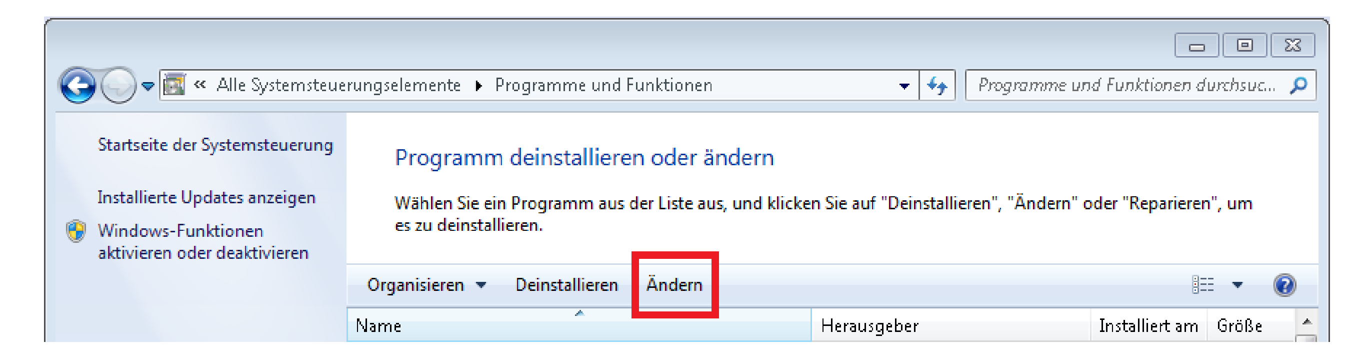
  Wählen Sie Avira Antivirus Suite aus und klicken Sie auf **Ändern**.

  Wählen Sie Im **Willkommens**-Dialogfeld des Programms die Option **Programm ändern**. Sie werden durch die Änderungsinstallation geführt.

Verwandte Themen:
Komponenten für die Installation wählen

3.7.2 Installation unter Windows 7 ändern

Sie haben die Möglichkeit, einzelne Programmkomponenten der aktuellen Avira Antivirus Suite Installation hinzuzufügen oder zu entfernen (siehe Komponenten für die Installation wählen).



Wenn Sie Programmkomponenten der aktuellen Installation hinzufügen oder entfernen möchten, können Sie in der **Windows-Systemsteuerung** die Option **Software** zum **Ändern/Entfernen von Programmen** verwenden.

- Öffnen Sie über das Windows **Start**-Menü die **Systemsteuerung**.

  Doppelklicken Sie auf **Programme und Funktionen**.

  Wählen Sie Avira Antivirus Suite aus und klicken Sie auf **Ändern**.

  Wählen Sie Im **Willkommens**-Dialogfeld des Programms die Option **Programm ändern**. Sie werden durch die Änderungsinstallation geführt.

Verwandte Themen:
Komponenten für die Installation wählen

3.7.3 Installation unter Windows XP ändern

Sie haben die Möglichkeit, einzelne Programmkomponenten der aktuellen Avira Antivirus Suite Installation hinzuzufügen oder zu entfernen (siehe Komponenten für die Installation wählen).

Wenn Sie Programmkomponenten der aktuellen Installation hinzufügen oder entfernen möchten, können Sie in der **Windows-Systemsteuerung** die Option **Software** zum **Ändern/Entfernen** von Programmen verwenden.

- Öffnen Sie die **Systemsteuerung** über **Start > Einstellungen** in Windows.

  Doppelklicken Sie auf **Programme hinzufügen oder entfernen**.

  Wählen Sie Avira Antivirus Suite aus und klicken Sie auf **Ändern**.

  Wählen Sie Im **Willkommens**-Dialogfeld des Programms die Option **Programm ändern**. Sie werden durch die Änderungsinstallation geführt.

Verwandte Themen:
Komponenten für die Installation wählen

3.8 Avira Antivirus Suite deinstallieren

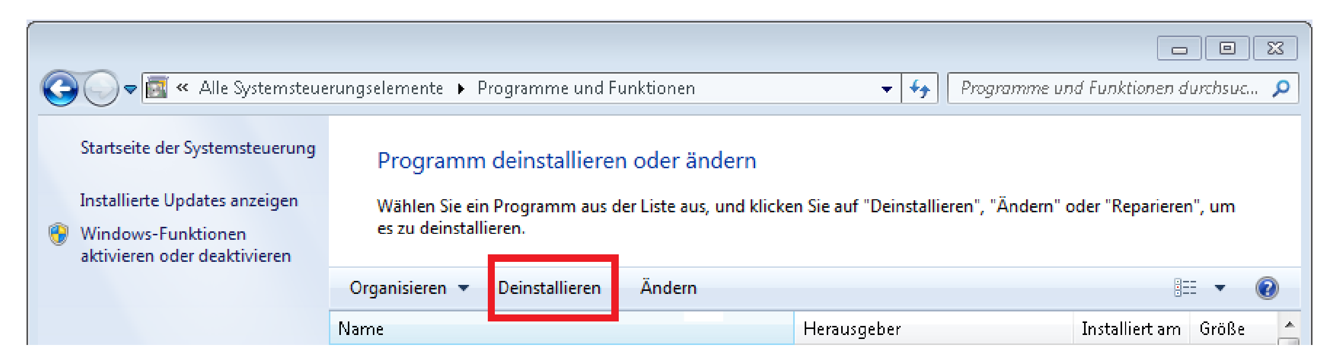
Sollten Sie Avira Antivirus Suite einmal deinstallieren wollen, gehen Sie wie folgt vor:

- Avira Antivirus Suite unter Windows 8 deinstallieren
- Avira Antivirus Suite unter Windows 7 deinstallieren
- Avira Antivirus Suite unter Windows XP deinstallieren



3.8.1 Avira Antivirus Suite unter Windows 8 deinstallieren

Um Avira Antivirus Suite von Ihrem Computer zu deinstallieren, verwenden Sie die Option **Programme und Funktionen** in der Windows-Systemsteuerung.



- Klicken Sie mit der rechten Maustaste auf den Bildschirm.

  Das Symbol **Alle Apps** erscheint.

  Klicken Sie auf das Symbol und suchen Sie unter *Apps - System* nach **Systemsteuerung**.

  Doppelklicken Sie auf das Symbol **Systemsteuerung**.

  Klicken Sie auf **Programme - Programm deinstallieren**.

  Klicken Sie auf **Programme und Funktionen - Programm deinstallieren**.

  Wählen Sie Avira Antivirus Suite aus der Liste aus und klicken Sie auf **Deinstallieren**.

  Wenn Sie gefragt werden, ob Sie diese Anwendung und alle ihre Komponenten vollständig entfernen möchten, bestätigen Sie mit **Ja**.

  Alle Komponenten des Programms werden entfernt.

  Klicken Sie auf **Fertig stellen**, um die Deinstallation abzuschließen.

  Wenn ein Dialogfenster mit der Empfehlung Ihren Computer neu zu starten erscheint, bestätigen Sie mit **Ja**.

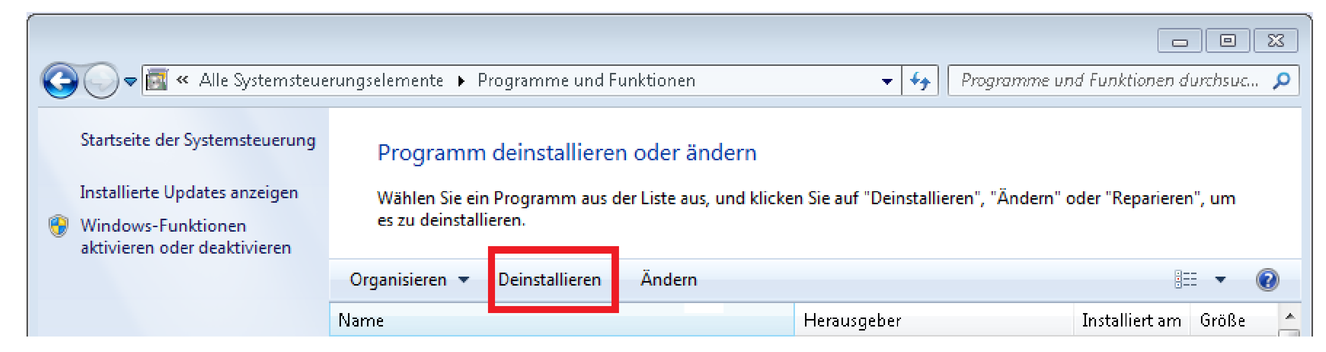
  Avira Antivirus Suite ist nun deinstalliert und alle Verzeichnisse, Dateien und Registry-Einträge des Programms werden gelöscht, wenn Ihr Computer neu gestartet wird.

> **Hinweis**
> Die Avira SearchFree Toolbar ist nicht in der Programm-Deinstallation enthalten, sondern muss separat deinstalliert werden.

3.8.2 Avira Antivirus Suite unter Windows 7 deinstallieren

Um Avira Antivirus Suite von Ihrem Computer zu deinstallieren, verwenden Sie die Option **Programme und Funktionen** in der Windows-Systemsteuerung.





- Öffnen Sie über das Windows **Start**-Menü die **Systemsteuerung**.

  Klicken Sie auf **Programme und Funktionen**.

  Wählen Sie Avira Antivirus Suite aus der Liste aus und klicken Sie auf **Deinstallieren**.

  Wenn Sie gefragt werden, ob Sie diese Anwendung und alle ihre Komponenten vollständig entfernen möchten, bestätigen Sie mit **Ja**.

  Alle Komponenten des Programms werden entfernt.

  Klicken Sie auf **Fertig stellen**, um die Deinstallation abzuschließen.

  Wenn ein Dialogfenster mit der Empfehlung Ihren Computer neu zu starten erscheint, bestätigen Sie mit **Ja**.

  Avira Antivirus Suite ist nun deinstalliert und alle Verzeichnisse, Dateien und Registry-Einträge des Programms werden gelöscht, wenn Ihr Computer neu gestartet wird.

> **Hinweis**
> Die Avira SearchFree Toolbar ist nicht in der Programm-Deinstallation enthalten, sondern muss separat deinstalliert werden.

3.8.3 Avira Antivirus Suite unter Windows XP deinstallieren

Um Avira Antivirus Suite von Ihrem Computer zu deinstallieren, verwenden Sie in der Windows-Systemsteuerung die Option **Programme ändern oder entfernen**.

- Öffnen Sie die **Systemsteuerung** über **Start > Einstellungen** in Windows.

  Doppelklicken Sie auf **Programme hinzufügen oder entfernen**.

  Wählen Sie Avira Antivirus Suite aus der Liste und klicken Sie auf **Entfernen**.

  Wenn Sie gefragt werden, ob Sie diese Anwendung und alle ihre Komponenten vollständig entfernen möchten, bestätigen Sie mit **Ja**.

  Alle Komponenten des Programms werden entfernt.

  Klicken Sie auf **Fertig stellen**, um die Deinstallation abzuschließen.

  Wenn ein Dialogfenster mit der Empfehlung Ihren Computer neu zu starten erscheint, bestätigen Sie mit **Ja**.



Avira Antivirus Suite ist nun deinstalliert und alle Verzeichnisse, Dateien und Registry-Einträge des Programms werden gelöscht, wenn Ihr Computer neu gestartet wird.

Hinweis
Die Avira SearchFree Toolbar ist nicht in der Programm-Deinstallation enthalten, sondern muss separat deinstalliert werden.

3.8.4 Die Avira SearchFree Toolbar deinstallieren

Die Avira SearchFree Toolbar deinstallieren

Sollten Sie Avira SearchFree Toolbar einmal deinstallieren wollen, gehen Sie wie folgt vor:

- Avira SearchFree Toolbar unter Windows 8 deinstallieren
- Avira SearchFree Toolbar unter Windows 7 deinstallieren
- Avira SearchFree Toolbar unter Windows XP deinstallieren
- Avira SearchFree Toolbar über den Webbrowser deinstallieren
- Avira SearchFree Toolbar über den Add-On Manager deinstallieren

Avira SearchFree Toolbar unter Windows 8 deinstallieren

So deinstallieren Sie Ihre Avira SearchFree Toolbar:

- Schließen Sie den Webbrowser.

Führen Sie einen Rechtsklick in einer der unteren Ecken des Bildschirms aus.

Das Symbol **Alle Apps** erscheint.

Klicken Sie das Symbol und suchen Sie in der Rubrik *Apps - System* nach **Systemsteuerung**.

Doppelklicken Sie das Symbol **Systemsteuerung**.

Klicken Sie **Programme - Programm deinstallieren**.

Klicken Sie **Programme und Features - Programm deinstallieren**.

Wählen Sie Avira SearchFree Toolbar plus Browser-Schutz aus der Liste und klicken Sie **Deinstallieren**.

Sie werden gefragt, ob Sie dieses Produkt wirklich deinstallieren wollen.

Bestätigen Sie mit **Ja**.

Avira SearchFree Toolbar plus Browser-Schutz wird deinstalliert und alle Verzeichnisse, Dateien und Registry-Einträge der Avira SearchFree Toolbar plus Browser-Schutz werden gelöscht, wenn Ihr Computer neu gestartet wird.



Avira SearchFree Toolbar unter Windows 7 deinstallieren

So deinstallieren Sie Ihre Avira SearchFree Toolbar:

- Schließen Sie Ihren Webbrowser.

  Öffnen Sie über das Windows **Start**-Menü die **Systemsteuerung**.

  Doppelklicken Sie auf **Programme und Funktionen**.

  Wählen Sie Avira SearchFree Toolbar plus Browser-Schutz aus der Liste und klicken Sie **Deinstallieren**.

  Sie werden gefragt, ob Sie dieses Produkt wirklich deinstallieren wollen.

  Bestätigen Sie mit **Ja**.

  Avira SearchFree Toolbar plus Browser-Schutz wird deinstalliert und alle Verzeichnisse, Dateien und Registry-Einträge der Avira SearchFree Toolbar plus Browser-Schutz werden gelöscht, wenn Ihr Computer neu gestartet wird.

Avira SearchFree Toolbar unter Windows XP deinstallieren

So deinstallieren Sie Ihre Avira SearchFree Toolbar:

- Schließen Sie Ihren Webbrowser.

  Öffnen Sie über das Windows-Menü **Start > Einstellungen** die **Systemsteuerung**.

  Doppelklicken Sie **Programme hinzufügen oder entfernen**.

  Wählen Sie Avira SearchFree Toolbar plus Browser-Schutz aus der Liste und klicken Sie **Entfernen**.

  Sie werden gefragt, ob Sie dieses Produkt wirklich deinstallieren wollen.

  Bestätigen Sie mit **Ja**.

  Avira SearchFree Toolbar plus Browser-Schutz wird deinstalliert und alle Verzeichnisse, Dateien und Registry-Einträge der Avira SearchFree Toolbar plus Browser-Schutz werden gelöscht, wenn Ihr Computer neu gestartet wird.

Avira SearchFree Toolbar über den Webbrowser deinstallieren

Sie haben außerdem die Möglichkeit, die Avira SearchFree Toolbar direkt im Browser zu deinstallieren. Diese Option steht nur für Firefox und Internet Explorer zur Verfügung:

- Öffnen Sie Ihren Webbrowser.

  Öffnen Sie in der Suchleiste das **Optionen**-Menü.

  Klicken Sie auf **Toolbar vom Webbrowser deinstallieren**.

  Wenn Sie gefragt werden, ob Sie dieses Produkt deinstallieren möchten, bestätigen Sie mit **Ja**.

  Sie werden nun aufgefordert, Ihren Webbrowser zu schließen.

  Schließen Sie den Webbrowser und klicken Sie auf **Wiederholen**.



Avira SearchFree Toolbar plus Browser-Schutz wird deinstalliert und alle Verzeichnisse, Dateien und Registry-Einträge der Avira SearchFree Toolbar plus Browser-Schutz werden gelöscht, wenn Ihr Computer neu gestartet wird.

> **Hinweis**
> Um die Avira SearchFree Toolbar zu deinstallieren, muss die Toolbar im Add-On Manager aktiviert sein.

Avira SearchFree Toolbar über den Add-On Manager deinstallieren

Da die Toolbar als Add-On installiert wird, kann sie auch als solches deinstalliert werden:

Firefox

- Klicken Sie **Tools > Add-ons > Erweiterungen**. Dort können Sie das Add-On von Avira verwalten: d.h. ein- oder ausschalten und deinstallieren.

Internet Explorer

- Klicken Sie auf **Add-ons verwalten > Symbolleisten und Erweiterungen**. Dort können Sie das Add-On von Avira sowohl ein- und ausschalten als auch deinstallieren.

Chrome

- Mit einem Klick auf **Optionen > Erweiterungen** verwalten Sie das Avira Add-On. Dieses ermöglicht Ihnen, die Toolbar ein- oder auszuschalten oder zu deinstallieren.



4. Überblick über Avira Antivirus Suite

In diesem Kapitel erhalten Sie einen Überblick über die Funktionalitäten und die Bedienung Ihres Avira Produkts.

- siehe Kapitel Oberfläche und Bedienung
- siehe Kapitel Avira SearchFree Toolbar
- siehe Kapitel So wird es gemacht

4.1 Oberfläche und Bedienung

Sie bedienen Ihr Avira Produkt über drei Oberflächenelemente des Programms:

- Control Center: Überwachung und Steuerung des Avira Produkts
- Konfiguration: Konfiguration des Avira Produkts
- Tray Icon im Systemtray der Taskleiste: Öffnen des Control Center und weitere Funktionen

4.1.1 Control Center

Das Control Center dient zur Überwachung des Schutzstatus Ihres Computersystems und zur Steuerung und Bedienung der Schutzkomponenten und Funktionen Ihres Avira Produkts.

Das Fenster des Control Centers gliedert sich in drei Bereiche: Die **Menüleiste**, der **Navigationsbereich** und das Detailfenster **Status**:

- **Menüleiste:** In den Menüs des Control Centers können Sie allgemeine Programmfunktionen aufrufen und Informationen zum Produkt abrufen.
- **Navigationsbereich:** Im Navigationsbereich können Sie einfach zwischen den einzelnen Rubriken des Control Centers wechseln. Die einzelnen Rubriken enthalten Informationen und Funktionen der Programmkomponenten und sind in der Navigationsleiste nach Aufgabenbereichen angeordnet. Beispiel: Aufgabenbereich *PC SICHERHEIT* - Rubrik **Echtzeit-Scanner**.
- **Status:** Im Startbildschirm **Status** sehen Sie auf einen Blick, ob Ihr Computer ausreichend geschützt ist und haben sofort einen Überblick, welche Module aktiv sindund die letzte Systemprüfung durchgeführt wurden. Im Fenster **Status** befinden sich die Schaltflächen zur Ausführung von Funktionen bzw. Aktionen, wie etwa das Ein- oder Ausschalten des **Echtzeit-Scanners**.

Starten und beenden von Control Center

Sie haben folgende Möglichkeiten das Control Center zu starten:

- Mit Doppelklick auf das Programm-Icon auf Ihrem Desktop

- Über den Programm-Eintrag im Menü **Start > Programme**.
- Über das Tray Icon Ihres Avira Produkts.

Sie beenden das Control Center über den Menübefehl **Beenden** im Menü **Datei**, oder indem Sie auf das Schließen-Kreuz im Control Center klicken.

Control Center bedienen

So navigieren Sie im Control Center:

- Klicken Sie in der Navigationsleiste auf einen Aufgabenbereich unterhalb einer Rubrik.
  - ↳ Der Aufgabenbereich wird mit weiteren Funktions- und Konfigurationsmöglichkeiten im Detailfenster angezeigt. Der Aufgabenbereich wird mit weiteren Funktions- und Konfigurationsmöglichkeiten im Detailfenster angezeigt.
- Klicken Sie ggf. einen anderen Aufgabenbereich an, um diesen im Detailfenster anzuzeigen.

> **Hinweis**
> Die Tastaturnavigation in der Menüleiste aktivieren Sie mit Hilfe der [**Alt**]-Taste. Ist die Navigation aktiviert, können Sie sich mit den **Pfeiltasten** innerhalb des Menüs bewegen. Mit der **Enter**-Taste aktivieren Sie den aktuell markierten Menüpunkt.
> Um Menüs im Control Center zu öffnen, zu schließen oder in den Menüs zu navigieren können Sie auch Tastenkombinationen verwenden: [**Alt**]-Taste + unterstrichener Buchstabe im Menü oder Menübefehl. Halten Sie die [**Alt**]-Taste gedrückt, wenn Sie aus einem Menü einen Menübefehl oder ein Untermenü aufrufen möchten.

So bearbeiten Sie Daten oder Objekte, die im Detailfenster angezeigt werden:

- Markieren Sie die Daten oder Objekte, die Sie bearbeiten möchten.

  Um mehrere Elemente zu markieren, halten Sie die **Strg**-Taste oder die **Umsch**-Taste (Auswahl untereinander stehender Elemente) gedrückt, während Sie die Elemente auswählen.
- Klicken Sie auf die gewünschte Schaltfläche in der oberen Leiste des Detailfensters, um das Objekt zu bearbeiten.

Control Center im Überblick

- **Status**: Im Startbildschirm **Status** finden Sie alle Rubriken, mit denen Sie die Funktionsfähigkeit des Programms überwachen können (siehe Status).
  - Das Fenster **Status** bietet die Möglichkeit auf einen Blick zu sehen, welche Module aktiv sind und gibt Informationen über das letzte durchgeführte Update.



- *PC SICHERHEIT*: Hier finden Sie die Komponenten, mit denen Sie Dateien auf Ihrem Computersystem auf Viren und Malware prüfen.
  - Die Rubrik System-Scanner bietet Ihnen die Möglichkeit, die Direktsuche auf einfache Art und Weise zu konfigurieren bzw. zu starten. Vordefinierte Profile ermöglichen einen Suchlauf mit bereits angepassten Standardoptionen. Genau so ist es möglich mit Hilfe der Manuellen Auswahl (wird gespeichert) bzw. durch die Erstellung benutzerdefinierter Profile, die Suche nach Viren und unerwünschten Programmen auf Ihre persönlichen Bedürfnisse anzupassen.
  - Die Rubrik Echtzeit-Scanner zeigt Ihnen Informationen zu überprüften Dateien, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".
- *INTERNET SICHERHEIT*: Hier finden Sie die Komponenten, mit denen Sie Ihr Computersystem vor Viren und Malware aus dem Internet sowie vor unerwünschten Netzzugriffen schützen.
  - Die Rubrik FireWall bietet Ihnen die Möglichkeit, die Grundeinstellungen der FireWall zu konfigurieren. Es werden Ihnen außerdem die aktuelle Datenübertragungsrate und alle aktiven Anwendungen angezeigt, die eine Netzwerkverbindung verwenden.
  - Die Rubrik Browser-Schutz zeigt Ihnen Informationen zu überprüften URLs und gefundenen Viren, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".
  - Die Rubrik Email-Schutz zeigt Ihnen die vom Email-Schutz überprüften Emails, deren Eigenschaften sowie weitere statistische Daten. Zudem haben Sie die Möglichkeit Email-Adressen zukünftig von der Überprüfung auf Malware auszuschließen.
- *KINDER SCHUTZ*: Hier finden Sie Werkzeuge, mit denen Sie ein sicheres Web-Erlebnis für Ihre Kinder ermöglichen.
  - Soziale Netzwerke: Die Rubrik Soziale Netzwerke leitet Sie zur Avira Kinderschutz für soziale Netzwerke Anwendung weiter. Avira Kinderschutz für soziale Netzwerke informiert Eltern über die Online-Aktivitäten ihrer Kinder. Das System prüft die Konten der sozialen Netzwerke auf Kommentare, Fotos usw., die dem Ruf ihres Kindes schaden könnten oder die darauf hinweisen könnten, dass Ihr Kind gefährdet ist.
- *MOBILER SCHUTZ*: Über die Kategorie Avira Free Android Security können Sie online auf Ihre Android-Geräte zugreifen.
  - Mit Avira Free Android Security verwalten Sie all Ihre Geräte, die mit dem Android-Betriebssystem arbeiten.
- *VERWALTUNG*: Hier finden Sie Werkzeuge, mit denen Sie verdächtige oder von Viren betroffene Dateien isolieren und administrieren sowie wiederkehrende Aufgaben planen können.
  - Hinter der Rubrik Quarantäne verbirgt sich der so genannte Quarantänemanager. Die zentrale Stelle für bereits in Quarantäne gestellte Dateien oder aber für



verdächtige Dateien, die Sie in Quarantäne stellen möchten. Zudem besteht die Möglichkeit, eine ausgewählte Datei per Email an das Avira Malware Research Center zu senden.

- Die Rubrik Planer bietet Ihnen die Möglichkeit, zeitlich gesteuerte Prüf- und Update-Aufträge sowie Backup-Aufträge zu erstellen und bestehende Aufträge anzupassen bzw. zu löschen.
- Die Rubrik Berichte bietet Ihnen die Möglichkeit, sich die Ergebnisse der durchgeführten Aktionen anzusehen.
- Die Rubrik Ereignisse bietet Ihnen die Möglichkeit, sich über die Ereignisse zu informieren, die von den Modulen des Programms erzeugt werden.

4.1.2 Konfiguration

In der Konfiguration können Sie Einstellungen für Ihr Avira Produkt vornehmen. Nach der Installation ist Ihr Avira Produkt mit Standardeinstellungen konfiguriert, die gewährleisten, dass Ihr Computersystem optimal geschützt ist. Dennoch können Ihr Computersystem oder Ihre Anforderungen an Ihr Avira Produkt Besonderheiten aufweisen, so dass Sie die Schutzkomponenten des Programms anpassen möchten.

Die Konfiguration hat den Aufbau eines Dialogfensters: Mit den Schaltflächen **OK** oder **Übernehmen** speichern Sie Ihre in der Konfiguration vorgenommenen Einstellungen, mit **Abbrechen** verwerfen Sie Ihre Einstellungen, mit der Schaltfläche **Standardwerte** können

Sie die Einstellungen in der Konfiguration auf die Standardwerte zurücksetzen. In der linken Navigationsleiste können Sie einzelne Konfigurationsrubriken anwählen.

Aufrufen der Konfiguration

Sie haben mehrere Möglichkeiten die Konfiguration aufzurufen:

- Über die Windows Systemsteuerung.
- Über das Windows Sicherheitscenter - ab Windows XP Service Pack 2.
- Über das Tray Icon Ihres Avira Programms.
- Im Control Center über den Menüpunkt Extras > Konfiguration.
- Im Control Center über die Schaltfläche Konfiguration.

> **Hinweis**
> Wenn Sie die Konfiguration über die Schaltfläche **Konfiguration** im Control Center aufrufen, gelangen Sie in das Konfigurationsregister der Rubrik, die im Control Center aktiv ist.

Konfiguration bedienen

Sie navigieren innerhalb des Konfigurationsfensters wie im Windows Explorer:

- Klicken Sie einen Eintrag in der Baumstruktur an, um diese Konfigurationsrubrik im Detailfenster anzuzeigen.
- Klicken Sie auf das Plus-Zeichen vor einem Eintrag, um die Konfigurationsrubrik zu erweitern und untergeordnete Konfigurationsrubriken in der Baumstruktur anzuzeigen.
- Um untergeordnete Konfigurationsrubriken zu verbergen, klicken Sie auf das Minus-Zeichen vor der erweiterten Konfigurationsrubrik.

> **Hinweis**
> Um in der Konfiguration Optionen zu aktivieren oder deaktivieren und Schaltflächen zu drücken, können Sie auch die Tastenkombinationen verwenden: [**Alt**]-Taste + unterstrichener Buchstabe im Optionsnamen oder der Schaltflächenbezeichnung.

Wenn Sie Ihre Einstellungen in der Konfiguration übernehmen möchten:

- Klicken Sie auf die Schaltfläche **OK**.

  ↳ Das Konfigurationsfenster wird geschlossen und die Einstellungen werden übernommen.

  \- ODER -

  Klicken Sie auf die Schaltfläche **Übernehmen**.

↳ Die Einstellungen werden übernommen. Das Konfigurationsfenster bleibt geöffnet.

Wenn Sie die Konfiguration beenden möchten ohne Ihre Einstellungen zu übernehmen:

- Klicken Sie auf die Schaltfläche **Abbrechen**.

  ↳ Das Konfigurationsfenster wird geschlossen, und die Einstellungen werden verworfen.

Wenn Sie alle Einstellungen in der Konfiguration auf Standardwerte zurücksetzen möchten:

- Klicken Sie auf **Standardwerte**.

  ↳ Alle Einstellungen in der Konfiguration werden auf Standardwerte zurückgesetzt. Alle Änderungen und alle eigenen Einträge gehen beim Zurücksetzen auf die Standardwerte verloren.

Konfigurationsoptionen im Überblick

Sie haben folgende Konfigurationsoptionen:

- **System-Scanner**: Konfiguration der Direktsuche
  - Suchoptionen
  - Aktion bei Fund
  - Optionen bei Suche in Archiven
  - Ausnahmen der Direktsuche
  - Heuristik der Direktsuche
  - Einstellung der Reportfunktion
- **Echtzeit-Scanner**: Konfiguration der Echtzeitsuche
  - Suchoptionen
  - Aktion bei Fund
  - Weitere Aktionen
  - Ausnahmen der Echtzeitsuche
  - Heuristik der Echtzeitsuche
  - Einstellung der Reportfunktion
- **Update**: Konfigurationen der Update-Einstellungen
  - Einstellung der Produktupdates
  - Neustart Einstellungen
  - Download über Webserver
- **Browser-Schutz**: Konfiguration des Browser-Schutzes
  - Suchoptionen, Aktivierung und Deaktivierung des Browser-Schutzes
  - Aktion bei Fund



  - Gesperrte Zugriffe: Unerwünschte Dateitypen und MIME-Typen, Web-Filter für bekannte unerwünschte URLS (Malware, Phishing etc.)
  - Ausnahmen der Suche des Browser Schutzes: URLs, Dateitypen, MIME-Typen
  - Heuristik des Browser-Schutzes
  - Einstellung der Reportfunktion
- **Email-Schutz**: Konfiguration des Email-Schutzes
  - Suchoptionen: Aktivierung der Überwachung von POP3-Konten, IMAP-Konten, ausgehenden Emails (SMTP)
  - Aktion bei Fund
  - Weitere Aktionen
  - Heuristik der Suche des Email Schutzes
  - Ausnahmen der Suche des Email-Schutzes
  - Konfiguration des Zwischenspeichers, Zwischenspeicher leeren
  - Einstellung der Reportfunktion
- **Allgemeines**:
  - Erweiterte Gefahrenkategorien für Direkt- und Echtzeitsuche
  - Erweiterter Schutz: ProActiv und Cloud-Sicherheit aktivieren
  - Anwendungsfilter: Anwendungen blockieren oder erlauben
  - Kennwortschutz für den Zugriff auf das Control Center und die Konfiguration
  - Sicherheit: Autorun Funktionen blockieren, Windows hosts-Datei sperren, Produktschutz
  - WMI: WMI-Unterstützung aktivieren
  - Konfiguration der Ereignis-Protokollierung
  - Konfiguration der Bericht-Funktionen
  - Einstellung der verwendeten Verzeichnisse
  - Konfiguration von akustischen Warnungen bei Malware-Fund

4.1.3 Tray Icon

Nach der Installation sehen Sie das Tray Icon Ihres Avira Produkts im Systemtray der Taskleiste:

Symbol	Beschreibung
	Avira Echtzeit-Scanner ist aktiviert
	Avira Echtzeit-Scanner ist deaktiviert

Das Tray Icon zeigt den Status des Echtzeit-Scanners an.



Über das Kontextmenü des Tray Icons sind zentrale Funktionen Ihres Avira Produkts schnell zugänglich. Um das Kontextmenü aufzurufen, klicken Sie mit der rechten Maustaste auf das Tray Icon.

Einträge im Kontextmenü

- **Echtzeit-Scanner aktivieren**: Aktiviert bzw. deaktiviert den Avira Echtzeit-Scanner.
- **Email-Schutz aktivieren**: Aktiviert bzw. deaktiviert den Avira Email-Schutz.
- **Browser-Schutz aktivieren**: Aktiviert bzw. deaktiviert den Avira Browser-Schutz.
  - **Windows Firewall aktivieren**: Aktiviert bzw. deaktiviert die Windows Firewall (diese Funktion ist erst ab Windows 8 verfügbar).
- **Avira Antivirus Suite starten**: Öffnet das Control Center.
- **Avira Antivirus Suite** konfigurieren: Öffnet die Konfiguration.
- **Meine Meldungen**: Öffnet ein Slide-Up mit aktuellsten Meldungen zu Ihrem Avira Produkt.
- **Meine Kommunikationseinstellungen**: Öffnet das Abo-Center für Produktmitteilungen
- **Update starten:** Startet ein Update.
- **Hilfe**: Öffnet die Online-Hilfe.
- **Experts Market**: öffnet die Webseite Experts Market - Hilfe anfordern. Dort können Sie um Hilfe bitten oder anderen Anwendern Ihre Hilfe anbieten.
- **Über Avira Antivirus Suite:** Öffnet ein Dialogfenster mit Informationen zu Ihrem Avira Produkt: Produktinformationen, Versionsinformationen, Lizenzinformationen.
- **Avira im Internet**: Öffnet das Avira Webportal im Internet. Voraussetzung ist, dass Sie einen aktiven Zugang zum Internet haben.

> **Hinweis**
> Die Benutzerkontensteuerung (UAC) benötigt Ihre Zustimmung zur Aktivierung oder Deaktivierung der Echtzeit-Scanner, Browser-Schutz und Email-Schutz Dienste in Betriebssystemen ab Windows Vista.

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar beinhaltet zwei Hauptkomponenten: Avira SearchFree und die schon bekannte Toolbar.

Die neue Avira SearchFree Toolbar wird als ein Add-on installiert. Beim ersten Aufrufen des Browsers (bei Internet Explorer und Firefox) werden Sie gefragt, ob Sie zulassen möchten, dass das Programm Avira SearchFree Toolbar Ihren Browser modifiziert. Sie müssen akzeptieren, um eine erfolgreiche Installation von Avira SearchFree Toolbar abzuschließen.



Avira SearchFree ist die neue Suchmaschine von Avira und enthält ein klickbares Avira Logo, das zu der Avira Webseite führt, sowie Web- und Bildkanäle. Sie ermöglicht Avira-Benutzern eine umfangreiche und sichere Suche.

Die Toolbar wird in Ihren Webbrowser integriert und besteht aus einem Suchfeld, einem mit der Avira Webseite verlinkten Avira Logo, zwei Statusanzeigen, drei Widgets und dem Menü **Optionen**.

- Suchleiste
  Nutzen Sie die Suchleiste, um schnell und kostenlos mithilfe der Avira SearchFree Suchmaschine das Internet zu durchsuchen.
- Statusanzeige
  Die Statusanzeigen geben Aufschluss über den Status des Browser-Schutzes und den aktuellen Update-Status Ihres Avira Produkts und helfen Ihnen, zu erkennen, welche Aktionen Sie ggf. zum Schutz Ihres PCs durchführen sollten.
- Widgets
  Avira gibt Ihnen direkten Zugang zu wichtigen Funktionen rund ums Internet, z.B. Ihre Facebook-Nachrichten oder Ihr Email-Postfach. Mit nur einem Klick haben Sie direkten Zugriff auf Facebook und zu Ihren Emails, oder können die sichere Internetsuche aktivieren (nur Firefox und Internet Explorer).
- Optionen
  Mithilfe des Optionen-Menüs können Sie auf die Toolbar-Optionen zugreifen, den Suchverlauf löschen, Hilfe und Informationen zur Toolbar aufrufen und die Avira SearchFree Toolbar auch direkt über den Webbrowser deinstallieren (nur Firefox und Internet Explorer).

4.2.1 Verwendung

Suchleiste

Mithilfe der Suchleiste können Sie das Internet nach einem oder mehreren beliebigen Begriffen durchsuchen.

Geben Sie dafür den Begriff in das Suchfeld ein und drücken Sie danach die **Enter**-Taste oder klicken Sie auf **Suche**. Die Avira SearchFree Suchmaschine durchsucht nun das Internet für Sie und zeigt dann alle Treffer im Browser-Fenster an.

Wie Sie Avira SearchFree im Internet Explorer, Firefox und Chrome Ihren Wünschen entsprechend konfigurieren können, finden Sie unter **Optionen.**

Statusanzeige

Browser-Schutz

Zur Bestimmung des Sicherheitsstatus Ihres Computers, können Sie folgende Icons und Meldungen nutzen:

Browser-Schutz

Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung: *Avira Browser-Schutz ist aktiv. Sie können jetzt sicher im Internet surfen.*

Das bedeutet, dass keine weiteren Aktionen erforderlich sind.

Browser-Schutz

Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung: *Avira Browser-Schutz ist deaktiviert. Klicken Sie auf den Link, um zu erfahren, wie Sie ihn aktivieren können.*

↳ Sie werden auf einen Artikel unserer Wissensdatenbank weitergeleitet.

Kein Browser-Schutz

Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung:

- *Sie haben Avira Browser-Schutz noch nicht installiert. Klicken Sie auf den Link, um mehr darüber zu erfahren, wie Sie sicher im Internet surfen können.*

  Das bedeutet, dass Sie entweder Avira Antivirus deinstalliert haben oder, dass es nicht richtig installiert wurde.

- *Browser-Schutz ist kostenlos in Avira Antivirus enthalten. Klicken Sie auf den Link, um mehr über seine Installation zu erfahren.*

  Das bedeutet, dass Sie Browser-Schutz nicht installiert, oder deinstalliert haben.

  ↳ In beiden Fällen werden Sie auf die Avira Webseite weitergeleitet, von der Sie Ihr Avira Produkt herunterladen können.

Fehler

Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung: *Avira hat einen Fehler gemeldet.*

- Klicken Sie auf das graue Symbol oder den Text, um zur Avira Support-Seite zu gelangen.

Widgets

Avira SearchFree Toolbar verfügt über 3 Widgets mit den wichtigsten Funktionen rund ums Internet: Facebook, Email und Browser-Sicherheit.

Facebook



Diese Funktion ermöglicht Ihnen, die Mitteilungen von Facebook direkt zu erhalten und so auf dem neuesten Stand zu bleiben.

Email

Wenn Sie auf das Email Symbol klicken, bekommen Sie eine Dropdown-Liste angezeigt, in der Sie zwischen den meistverwendeten Anbietern wählen können.

Browser-Sicherheit

Dieses Widget wurde von Avira entwickelt, um alle Internet-Sicherheitsoptionen besonders leicht erreichbar zu machen. Zur Zeit ist es nur für Firefox und Internet Explorer verfügbar. Es werden verschiedene Optionen angeboten, die je nach Browser anders heißen können:

- *Pop-up-Blocker*

Ist diese Option eingeschaltet, werden alle Pop-up-Fenster blockiert, wenn Sie im Internet surfen.

- *Cookie-Blocker*

Ist diese Option aktiviert, werden während des Browsens keine Cookies gespeichert.

- *Privater Modus (Firefox) / In Private Browsen (Internet Explorer)*

Ist diese Option eingeschaltet, hinterlassen Sie keine Spuren, wenn Sie im Internet surfen. Diese Option wird nicht für Internet Explorer 7 und 8 angeboten.

- *Neueste Chronik löschen (Firefox) / Browserverlauf löschen (Internet Explorer)*

Mit dieser Option löschen Sie alle Ihre bisherigen Internetaktivitäten.

Sicherheitsberater

Der Sicherheitsberater bietet Ihnen eine Sicherheitseinstufung während Sie im Internet navigieren.
So können Sie abschätzen, ob die Webseite die Sie gerade besuchen, ein hohes oder ein niedriges Risiko für Ihre Sicherheit birgt.
Dieses Widget bietet Ihnen weitere Informationen über die Webseite, wie z.B. wer der Domain-Besitzer ist oder warum eine Webseite in eine bestimmte Kategorie eingestuft wurde.
Es gibt drei Sicherheitsstufen: sicher, risikoarm und risikoreich.

Die Sicherheitsstufen werden in der Toolbar und in Ihren Suchergebnissen angezeigt, dargestellt in Form eines Avira Tray Icon mit verschiedenen Symbolen:

 *Sicher*

Ein grünes Häkchen für sichere Webseiten.

 *Risikoarm*

Ein gelbes Ausrufezeichen für Webseiten, die ein geringes Risiko darstellen.



 *Risikoreich*

Ein rotes Stopp-Schild für Webseiten, die ein hohes Risiko für Ihre Sicherheit bergen.

 *Gescheitert*

Ein graues Fragezeichen für Webseiten, deren Risiko nicht eingeschätzt werden kann.

 *Überprüfung läuft*

Dieses Zeichen wird erscheinen, während der Status verifiziert wird.

Spurenblocker

Mit dem Spurenblocker können Sie Nachverfolgungen stoppen, die Informationen über Sie sammeln während Sie im Internet surfen.
Das Widget erlaubt Ihnen zu wählen, welche Nachverfolgungen blockiert und welche zugelassen werden.

Die Unternehmen sind in drei Kategorien eingeteilt:

- Soziale Netzwerke
- Netzwerke
- Andere Unternehmen

4.2.2 Optionen

Die Avira SearchFree Toolbar ist mit Internet Explorer, Firefox und Google Chrome kompatibel und lässt sich in den Webbrowsern Ihren Wünschen entsprechend konfigurieren:

- Internet Explorer Konfigurationsoptionen
- Firefox Konfigurationsoptionen
- Chrome Konfigurationsoptionen

Internet Explorer

Im Internet Explorer Webbrowser stehen im Menü **Optionen** folgende Konfigurationsoptionen für die Avira SearchFree Toolbar zur Verfügung:

Toolbar-Optionen

Suche

Avira-Suchmaschine

Im Menü **Avira-Suchmaschine** können Sie auswählen, welche Suchmaschine für die Suchanfrage verwendet werden soll. Zur Verfügung stehen Suchmaschinen aus den

USA, Brasilien, Deutschland, Spanien, Europa, Frankreich, Italien, den Niederlanden, Russland und Großbritannien.

Suche öffnen in

Im Menü der Option **Suche öffnen in** können Sie auswählen, wo das Ergebnis einer Suchanfrage angezeigt werden soll, ob im **Aktuellen Fenster**, in einem **Neuen Fenster** oder auf einer **Neuen Registerkarte**.

Letzte Suchanfragen anzeigen

Ist die Option **Letzte Suchanfragen anzeigen** aktiviert, können Sie sich unterhalb des Texteingabefeldes der Suchleiste die bisher eingegebenen Suchbegriffe anzeigen lassen.

Suchverlauf beim Schließen des Browsers löschen

Aktivieren Sie die Option **Suchverlauf beim Schließen des Browsers löschen**, wenn Sie den Suchverlauf der bereits durchgeführten Suchen nicht speichern, sondern mit dem Schließen des Webbrowsers löschen möchten.

Weitere Optionen

Toolbar-Sprache

Unter **Toolbar-Sprache** können Sie die Sprache auswählen, in der die Avira SearchFree Toolbar angezeigt werden soll. Zur Verfügung stehen Englisch, Deutsch, Spanisch, Französisch, Italienisch, Portugiesisch und Niederländisch.

> **Hinweis**
> Die voreingestellte Sprache der Avira SearchFree Toolbar entspricht der Ihres Programmes, soweit verfügbar. Steht die Toolbar in Ihrer Sprache nicht zur Verfügung, ist die voreingestellte Sprache Englisch.

Schaltflächenbeschriftungen anzeigen

Deaktivieren Sie die Option **Schaltflächenbeschriftungen anzeigen**, wenn Sie den Text neben den Icons der Avira SearchFree Toolbar ausblenden möchten.

Suchverlauf löschen

Aktivieren Sie die Option **Suchverlauf löschen**, wenn Sie die bereits durchgeführte(n) Suche(n) nicht speichern, sondern sofort löschen möchten.

Hilfe

Klicken Sie auf **Hilfe**, um die Webseite mit den häufig gestellten Fragen (FAQ) zur Toolbar aufzurufen.



Deinstallieren

Sie können die Avira SearchFree Toolbar auch direkt im Internet Explorer deinstallieren: Deinstallation über den Webbrowser.

Info

Klicken Sie auf **Info**, um angezeigt zu bekommen, welche Version der Avira SearchFree Toolbar installiert ist.

Firefox

Im Firefox Webbrowser stehen im Menü **Optionen** folgende Konfigurationsoptionen für die Avira SearchFree Toolbar zur Verfügung:

Toolbar-Optionen

Suche

Avira-Suchmaschine

Im Menü **Avira-Suchmaschine** können Sie auswählen, welche Suchmaschine für die Suchanfrage verwendet werden soll. Zur Verfügung stehen Suchmaschinen aus den USA, Brasilien, Deutschland, Spanien, Europa, Frankreich, Italien, den Niederlanden, Russland und Großbritannien.

Letzte Suchanfragen anzeigen

Ist die Option **Letzte Suchanfragen anzeigen** aktiviert, können Sie sich die bisher eingegebenen Suchbegriffe anzeigen lassen, indem Sie auf den Pfeil in der Suchleiste klicken. Wählen Sie einen der Begriffe aus, wenn Sie sich das Suchergebnis erneut anzeigen lassen wollen.

Suchverlauf beim Schließen des Browsers löschen

Aktivieren Sie die Option **Suchverlauf beim Schließen des Browsers löschen**, wenn Sie den Suchverlauf der bereits durchgeführten Suchen nicht speichern, sondern mit dem Schließen des Webbrowsers löschen möchten.

Suchergebnisse von Ask anzeigen, wenn ich Stichwörter oder ungültige URL-Adressen in das Adressfeld des Browsers eingebe

Ist diese Option aktiviert, wird jedes Mal, wenn Sie Stichwörter oder eine ungültige URL-Adresse in das Adressfeld des Webbrowsers eintragen, eine Suchanfrage gestartet und das Suchergebnis angezeigt.

Weitere Optionen

Toolbar-Sprache

Unter **Toolbar-Sprache** können Sie die Sprache auswählen, in der die Avira SearchFree Toolbar angezeigt werden soll. Zur Verfügung stehen Englisch, Deutsch, Spanisch, Französisch, Italienisch, Portugiesisch und Niederländisch.

Hinweis
Die voreingestellte Sprache der Avira SearchFree Toolbar entspricht der Ihres Programmes, soweit verfügbar. Steht die Toolbar in Ihrer Sprache nicht zur Verfügung, ist die voreingestellte Sprache Englisch.

Schaltflächenbeschriftungen anzeigen

Deaktivieren Sie die Option **Schaltflächenbeschriftungen anzeigen**, wenn Sie den Text neben den Icons der Avira SearchFree Toolbar ausblenden möchten.

Suchverlauf löschen

Aktivieren Sie die Option **Suchverlauf löschen**, wenn Sie die bereits durchgeführte(n) Suche(n) nicht speichern, sondern sofort löschen möchten.

Hilfe

Klicken Sie auf **Hilfe**, um die Webseite mit den häufig gestellten Fragen (FAQ) zur Toolbar aufzurufen.

Deinstallieren

Sie können die Avira SearchFree Toolbar auch direkt im Internet Explorer deinstallieren: Deinstallation über den Webbrowser.

Info

Klicken Sie auf **Info**, um angezeigt zu bekommen, welche Version der Avira SearchFree Toolbar installiert ist.

Chrome

Im Google Chrome Webbrowser finden Sie alle Konfigurationsoptionen unterhalb des roten Avira-Schirms. Folgende Optionen stehen für die Avira SearchFree Toolbar zur Verfügung:

Hilfe

Klicken Sie auf **Hilfe**, um die Webseite mit den häufig gestellten Fragen (FAQ) zur Toolbar aufzurufen.

Anweisungen zum Deinstallieren

Hier finden Sie Links zu Deinstallationsanweisungen für Avira SeachFree Toolbar.



Info

Klicken Sie auf **Info**, um angezeigt zu bekommen, welche Version der Avira SearchFree Toolbar installiert ist.

Avira SearchFree Toolbar ein- und ausblenden

Dieser Menüpunkt schaltet die Avira SearchFree Toolbar, die sich im oberen Teil des Fensters befindet, ein- und aus.

4.2.3 Die Avira SearchFree Toolbar deinstallieren

Sollten Sie Avira SearchFree Toolbar einmal deinstallieren wollen, gehen Sie wie folgt vor:

- Avira SearchFree Toolbar unter Windows 8 deinstallieren
- Avira SearchFree Toolbar unter Windows 7 deinstallieren
- Avira SearchFree Toolbar unter Windows XP deinstallieren
- Avira SearchFree Toolbar über den Webbrowser deinstallieren
- Avira SearchFree Toolbar über den Add-On Manager deinstallieren

4.3 So wird es gemacht

In den "So wird es gemacht" Kapiteln erhalten Sie eine kurze Anleitung zur Lizenz- und Produktaktivierung sowie zu den wichtigsten Funktionen Ihres Avira Produkts. Die ausgewählten, kurzen Beiträge dienen dazu, Ihnen rasch einen Überblick über die Funktionalitäten Ihres Avira Produkts zu verschaffen. Sie ersetzen jedoch nicht die ausführlichen Erklärungen in den einzelnen Kapiteln dieser Hilfe.

4.3.1 Lizenz aktivieren

So aktivieren Sie die Lizenz Ihres Avira Produkts:

Mit der *.KEY*-Lizenzdatei aktivieren Sie Ihre Lizenz für Ihr Avira Produkt. Die Lizenzdatei erhalten Sie von Avira per Email. Die Lizenzdatei enthält die Lizenz für alle Produkte, die Sie bei einem Bestellvorgang bestellt haben.

Wenn Sie Ihr Avira Produkt noch nicht installiert haben:

- Speichern Sie die Lizenzdatei in einem lokalen Verzeichnis auf Ihrem Computer.
- Installieren Sie Ihr Avira Produkt.
- Geben Sie bei der Installation an, wo Sie die Lizenzdatei gespeichert haben.

Wenn Sie Ihr Avira Produkt bereits installiert haben:

- Doppelklicken Sie in Ihrem Dateimanager oder in der Aktivierungs-Email auf die Lizenzdatei und folgen Sie den Bildschirmanweisungen der sich öffnenden Lizenzverwaltung.

  - ODER -

  Wählen Sie im Control Center Ihres Avira Produkts den Menüpunkt **Hilfe > Lizenzmanagement**

> **Hinweis**
> Ab Windows Vista erscheint das Dialogfenster **Benutzerkontensteuerung**. Melden Sie sich ggf. als Administrator an. Klicken Sie auf **Fortsetzen**.

- Markieren Sie die Lizenzdatei und klicken Sie auf **Öffnen**.
  ↳ Eine Meldung erscheint.
- Bestätigen Sie mit **OK**.
  ↳ Die Lizenz ist aktiviert.
- Starten Sie Ihr System ggf. neu.

4.3.2 Produkt aktivieren

Um Ihr Avira Produkt zu aktivieren, haben Sie die folgenden Optionen:

- Aktivierung mit einer gültigen Volllizenz

  Zur Aktivierung des Programms mit einer Volllizenz benötigen Sie einen gültigen Aktivierungscode, über den die Daten Ihrer erworbenen Lizenz erfasst sind. Den Aktivierungscode haben Sie entweder per Email von uns erhalten oder er ist auf der Produktverpackung vermerkt.

- Aktivierung mit einer Evaluationslizenz

  Ihr Avira Produkt wird mit einer automatisch generierten Evaluationslizenz aktiviert, mit der Sie das Avira Produkt in einem begrenzten Zeitraum im vollen Funktionsumfang testen können.

> **Hinweis**
> Zur Produktaktivierung oder zur Beantragung einer Testlizenz benötigen Sie eine aktive Internetverbindung.
> Falls keine Verbindung zu den Avira Servern erstellt werden kann, prüfen Sie ggf. die Einstellungen in der genutzten Firewall: Bei der Produktaktivierung werden Verbindungen über das HTTP-Protokoll und Port 80 (Webkommunikation) und über das Verschlüsselungsprotokoll SSL und Port 443 genutzt. Stellen Sie sicher, dass Ihre Firewall, eingehende und ausgehende Daten nicht blockiert. Prüfen Sie zunächst, ob Sie über Ihren Webbrowser, Webseiten aufrufen können.

So aktivieren Sie Ihr Avira Produkt:

Wenn Sie Ihr Avira Produkt noch nicht installiert haben:

- Installieren Sie Ihr Avira Produkt.
  - ↳ Während der Installation werden Sie aufgefordert, eine Aktivierungsoption zu wählen
- **Produkt aktivieren** = Aktivierung mit einer gültigen Volllizenz
- **Produkt testen** = Aktivierung mit einer Evaluationslizenz
- Geben Sie für eine Aktivierung mit Volllizenz den Aktivierungscode an.
- Bestätigen Sie die Auswahl des Aktivierungsverfahrens mit **Weiter**.
- Geben Sie ggf. Ihre persönlichen Daten für eine Registrierung an und bestätigen Sie mit **Weiter**.
  - ↳ Im folgenden Dialogfenster werden Ihre Lizenzdaten angezeigt. Ihr Avira Produkt wurde aktiviert.
- Fahren Sie mit der Installation fort.

Wenn Sie Ihr Avira Produkt bereits installiert haben:

- Wählen Sie im Control Center den Menüpunkt **Hilfe > Lizenzmanagement**.
  - ↳ Es öffnet sich der Lizenz-Assistent, in dem Sie eine Aktivierungsoption wählen können. Die weiteren Schritte der Produktaktivierung sind identisch mit dem oben dargestellten Ablauf.

4.3.3 Automatisierte Updates durchführen

So legen Sie mit dem Avira Planer einen Auftrag an, mit dem Ihr Avira Produkt automatisiert aktualisiert wird:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Planer**.
- Klicken Sie auf das Symbol + **Neuen Auftrag mit dem Wizard erstellen**.
  - ↳ Das Dialogfenster **Name und Beschreibung des Auftrags** erscheint.
- Benennen Sie den Auftrag und beschreiben Sie ihn gegebenenfalls.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Art des Auftrags** wird angezeigt.
- Wählen Sie **Update-Auftrag** aus der Auswahlliste.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Zeitpunkt des Auftrags** erscheint.
- Wählen Sie, wann das Update ausgeführt werden soll:
- **Sofort**



- **Täglich**
- **Wöchentlich**
- **Intervall**
- **Einmalig**
- **Login**

> **Hinweis**
> Wir empfehlen, regelmäßig und häufig Updates durchzuführen. Das empfohlene Update-Intervall beträgt: 2 Stunden.

- Geben Sie je nach Auswahl ggf. den Termin an.
- Wählen Sie ggf. Zusatzoptionen (je nach Auftragsart verfügbar):

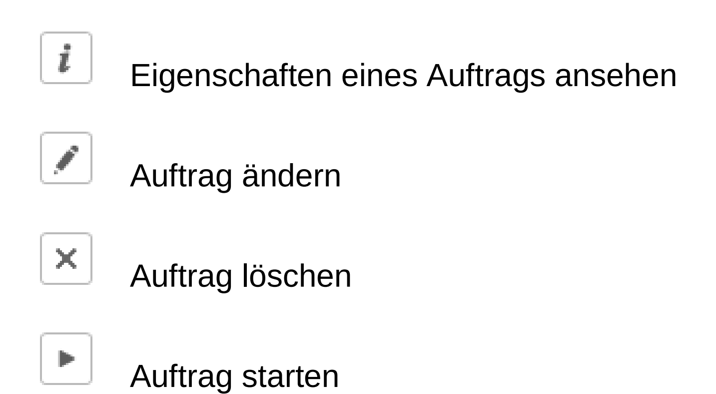
- **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**
  Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
- **Auftrag zusätzlich bei Internet-Verbindung starten (DFÜ)**
  Zusätzlich zur festgelegten Häufigkeit wird der Auftrag bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.

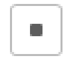
- Klicken Sie auf **Weiter**.
  ↳ Das Dialogfenster **Auswahl des Darstellungsmodus** erscheint.
- Wählen Sie den Darstellungsmodus des Auftragsfensters:

- **Unsichtbar**: kein Auftragsfenster
- **Minimiert**: nur Fortschrittsbalken
- **Maximiert**: gesamtes Auftragsfenster

- Klicken Sie auf **Fertig stellen**.
  ↳ Ihr neu angelegter Auftrag erscheint auf der Startseite der Rubrik *VERWALTUNG* **> Prüfen** als aktiviert (Häkchen).
- Deaktivieren Sie ggf. die Aufträge, die nicht ausgeführt werden sollen.

Über folgende Symbole können Sie Aufträge weiter bearbeiten:



 Auftrag stoppen

4.3.4 Ein Update manuell starten

Sie haben verschiedene Möglichkeiten ein Update manuell zu starten: Beim manuell gestarteten Update wird immer ein Update der Virendefinitionsdatei und der Suchengine durchgeführt. Ein Produktupdate erfolgt nur dann, wenn Sie in der Konfiguration unter PC Sicherheit > Update > Produktupdate die Option **Produktupdates herunterladen und automatisch installieren** aktiviert haben.

So starten Sie manuell ein Update Ihres Avira Produkts:

- Klicken Sie mit der rechten Maustaste auf das Avira Tray Icon in der Taskleiste und wählen Sie **Update starten**.

  \- ODER -

- Wählen Sie im Control Center die Rubrik **Status**, dann klicken Sie im Bereich **Letztes Update** auf den Link **Update starten**.

  \- ODER -

  Wählen Sie im Control Center im Menü **Update** den Menübefehl **Update starten**.

  ↳ Das Dialogfenster **Updater** erscheint.

Hinweis
Wir empfehlen, regelmäßige automatische Updates durchzuführen. Das empfohlene Update-Intervall beträgt: 2 Stunden.

Hinweis
Sie können ein manuelles Update auch direkt über das Windows Sicherheitscenter ausführen.

4.3.5 Direktsuche: Mit einem Suchprofil nach Viren und Malware suchen

Ein Suchprofil ist eine Zusammenstellung von Laufwerken und Verzeichnissen, die durchsucht werden sollen.

Sie haben folgende Möglichkeit über ein Suchprofil zu suchen:

- Vordefiniertes Suchprofil verwenden

  Wenn die vordefinierten Suchprofile Ihren Bedürfnissen entsprechen.

- Suchprofil anpassen und verwenden (manuelle Auswahl)

  Wenn Sie mit einem individualisierten Suchprofil suchen möchten.

- Neues Suchprofil erstellen und verwenden

Wenn Sie ein eigenes Suchprofil anlegen möchten.

Je nach Betriebssystem stehen für das Starten eines Suchprofils verschiedene Symbole zur Verfügung:

- Unter Windows XP:

  Mit diesem Symbol starten Sie die Suche über ein Suchprofil.
- Ab Windows Vista:

  Ab Microsoft Windows Vista hat das Control Center zunächst nur eingeschränkte Rechte z.B. für den Zugriff auf Verzeichnisse und Dateien. Bestimmte Aktionen und Dateizugriffe kann das Control Center nur mit erweiterten Administratorrechten ausführen. Diese erweiterten Administratorrechte müssen bei jedem Start einer Suche über ein Suchprofil erteilt werden.

  Mit diesem Symbol starten Sie eine eingeschränkte Suche über ein Suchprofil. Es werden nur die Verzeichnisse und Dateien durchsucht, für die das Betriebsystem die Zugriffsrechte erteilt hat.

  Mit diesem Symbol starten Sie die Suche mit erweiterten Administratorrechten. Nach einer Bestätigung werden alle Verzeichnisse und Dateien im gewählten Suchprofil durchsucht.

So suchen Sie mit einem Suchprofil nach Viren und Malware:

- Wählen Sie im Control Center die Rubrik *PC SICHERHEIT* **> System-Scanner**.

  ↳ Vordefinierte Suchprofile erscheinen.
- Wählen Sie eines der vordefinierten Suchprofile aus.

  -ODER-

  Passen Sie das Suchprofil **Manuelle Auswahl** an.

  -ODER-

  Erstellen Sie ein neues Suchprofil

- Klicken auf das Symbol (Windows XP: oder ab Windows Vista:).
- Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.

  ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

Wenn Sie ein Suchprofil anpassen möchten:

- Klappen Sie im Suchprofil **Manuelle Auswahl** den Dateibaum so weit auf, dass alle Laufwerke und Verzeichnisse geöffnet sind, die geprüft werden sollen

- Klick auf das **+** Zeichen: Nächste Verzeichnisebene wird angezeigt.
- Klick auf das **-** Zeichen: Nächste Verzeichnisebene wird verborgen.

- Markieren Sie die Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das jeweilige Kästchen der jeweiligen Verzeichnisebene

Sie haben folgende Möglichkeiten, Verzeichnisse auszuwählen:

- Verzeichnis einschließlich Unterverzeichnisse (schwarzes Häkchen)
- Nur Unterverzeichnisse in einem Verzeichnis (graues Häkchen, Unterverzeichnisse haben schwarze Häkchen)
- Kein Verzeichnis (kein Häkchen)

Wenn Sie ein neues Suchprofil erstellen möchten:

- Klicken Sie auf das Symbol **Neues Profil erstellen.**
  - ↳ Das Profil *Neues Profil* erscheint unterhalb der bisher vorhandenen Profile.
- Benennen Sie das Suchprofil ggf. um, indem Sie auf das Symbol klicken.
- Markieren Sie die Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das Kästchen der jeweiligen Verzeichnisebene.

Sie haben folgende Möglichkeiten, Verzeichnisse auszuwählen:

- Verzeichnis einschließlich Unterverzeichnisse (schwarzes Häkchen)
- Nur Unterverzeichnisse in einem Verzeichnis (graues Häkchen, Unterverzeichnisse haben schwarze Häkchen)
- Keine Verzeichnisse (kein Häkchen)

4.3.6 Direktsuche: Per Drag & Drop nach Viren und Malware suchen

So suchen Sie per Drag & Drop gezielt nach Viren und Malware:

✓ Das Control Center Ihres Avira Programms ist geöffnet.

- Markieren Sie die Datei oder das Verzeichnis, die/das geprüft werden soll.
- Ziehen Sie mit der linken Maustaste die markierte Datei oder das markierte Verzeichnis in das Control Center.
  - ↳ Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.
  - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

4.3.7 Direktsuche: Über das Kontextmenü nach Viren und Malware suchen

So suchen Sie über das Kontextmenü gezielt nach Viren und Malware:

- Klicken Sie (z.B. im Windows Explorer, auf dem Desktop oder in einem geöffneten Windows-Verzeichnis) mit der rechten Maustaste auf die Datei bzw. das Verzeichnis, die/das Sie prüfen wollen.
  - ↳ Das Kontextmenü des Windows Explorers erscheint.
- Wählen Sie im Kontextmenü **Ausgewählte Dateien mit Avira überprüfen**.
  - ↳ Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.

↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

4.3.8 Direktsuche: Automatisiert nach Viren und Malware suchen

> **Hinweis**
> Nach der Installation ist der Prüfauftrag *Vollständige Systemprüfung* im Planer angelegt: In einem empfohlenen Intervall wird automatisch eine vollständige Systemprüfung ausgeführt.

So legen Sie einen Auftrag an, der automatisiert nach Viren und Malware sucht:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Planer**.
- Klicken Sie auf das Symbol + **Neuen Auftrag mit dem Wizard erstellen**.
  ↳ Das Dialogfenster **Name und Beschreibung des Auftrags** erscheint.
- Benennen Sie den Auftrag und beschreiben Sie ihn gegebenenfalls.
- Klicken Sie auf **Weiter**.
  ↳ Das Dialogfenster **Art des Auftrags** erscheint.
- Wählen Sie den **Prüfauftrag**.
- Klicken Sie auf **Weiter**.
  ↳ Das Dialogfenster **Auswahl des Profils** erscheint.
- Wählen Sie, welches Profil durchsucht werden soll.
- Klicken Sie auf **Weiter**.
  ↳ Das Dialogfenster **Zeitpunkt des Auftrags** erscheint.
- Wählen Sie aus, wann der Suchlauf ausgeführt werden soll:

- **Sofort**
- **Täglich**
- **Wöchentlich**
- **Intervall**
- **Einmalig**
- **Login**

- Geben Sie je nach Auswahl ggf. den Termin an.
- Wählen Sie ggf. folgende Zusatzoption (je nach Auftragsart verfügbar): **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**
  ↳ Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
- Klicken Sie auf **Weiter**.

↳ Das Dialogfenster **Auswahl des Darstellungsmodus** erscheint.

- Wählen Sie den Darstellungsmodus des Auftragsfensters:

- **Unsichtbar**: kein Auftragsfenster
- **Minimiert**: nur Fortschrittsbalken
- **Maximiert**: gesamtes Auftragsfenster

- Wählen Sie die Option **Computer herunterfahren, wenn der Auftrag ausgeführt wurde**, wenn Sie möchten, dass der Rechner automatisch heruntergefahren wird, sobald der Auftrag ausgeführt und beendet wurde.

  Die Option ist nur im minimierten oder maximierten Darstellungsmodus verfügbar.

- Klicken Sie auf **Fertig stellen**.

  ↳ Ihr neu angelegter Auftrag erscheint auf der Startseite der Rubrik *VERWALTUNG* **> Planer** als aktiviert (Häkchen).

- Deaktivieren Sie ggf. die Aufträge, die nicht ausgeführt werden sollen.

Über folgende Symbole können Sie Aufträge weiter bearbeiten:

Eigenschaften zu einem Auftrag ansehen

Auftrag ändern

Auftrag löschen

Auftrag starten

Auftrag stoppen

4.3.9 Direktsuche: Gezielt nach aktiven Rootkits suchen

Um nach aktiven Rootkits zu suchen, nutzen Sie das vordefinierte Suchprofil **Suche nach Rootkits und aktiver Malware**.

So suchen Sie gezielt nach aktiven Rootkits:

- Wählen Sie im Control Center die Rubrik *PC SICHERHEIT* **> System-Scanner**.

  ↳ Vordefinierte Suchprofile erscheinen.

- Wählen Sie das vordefinierte Suchprofil **Suche nach Rootkits und aktiver Malware**.

- Markieren Sie ggf. weitere Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das Kästchen der Verzeichnisebene.



- Klicken Sie auf das Symbol (Windows XP: oder Windows Vista:).
  - ↳ Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.
  - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

4.3.10 Auf gefundene Viren und Malware reagieren

Für die einzelnen Schutzkomponenten Ihres Avira Produkts können Sie in der **Konfiguration** jeweils unter der Rubrik **Aktion bei Fund** einstellen, wie Ihr Avira Produkt bei einem Fund eines Virus oder unerwünschten Programms reagiert.

Bei der ProActiv-Komponente des Echtzeit-Scanners bestehen keine konfigurierbaren Aktionsoptionen: Ein Fund wird immer im Fenster **Echtzeit-Scanner: Verdächtiges Verhalten einer Anwendung** gemeldet.

Aktionsoptionen beim System-Scanner:

Interaktiv

Im interaktiven Aktionsmodus werden Funde der Suche des System-Scanners in einem Dialogfenster gemeldet. Diese Einstellung ist standardmäßig aktiviert.

Bei der **Suche des System-Scanners** erhalten Sie beim Abschluss der Suche eine Warnmeldung mit einer Liste der gefundenen betroffenen Dateien. Sie haben die Möglichkeit, über das Kontextmenü eine auszuführende Aktion für die einzelnen betroffenen Dateien auszuwählen. Sie können die gewählten Aktionen für alle betroffenen Dateien ausführen oder den System-Scanner beenden.

Automatisch

Im automatischen Aktionsmodus wird bei einem Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben.

Aktionsoptionen beim Echtzeit-Scanner:

Interaktiv

Im interaktiven Aktionsmodus wird der Datenzugriff verweigert und eine Desktop-Benachrichtigung angezeigt. In der Desktop-Benachrichtigung können Sie die gefundene Malware entfernen oder über die Schaltfläche **Details** zur weiteren Virenbehandlung an die Komponente System-Scanner übergeben. Der System-Scanner meldet den Fund in einem Fenster, in dem Sie über ein Kontextmenü verschiedene Optionen zur Behandlung der betroffenen Datei haben (siehe Fund > System-Scanner):



Automatisch

Im automatischen Aktionsmodus wird beim Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben.

Aktionsoptionen beim Email-Schutz, Browser-Schutz:

Interaktiv

Im interaktiven Aktionsmodus erscheint bei einem Fund eines Virus bzw. unerwünschten Programms ein Dialogfenster, in dem Sie auswählen können, was mit dem betroffenen Objekt weiter geschehen soll. Diese Einstellung ist standardmäßig aktiviert.

Automatisch

Im automatischen Aktionsmodus wird bei einem Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben.

Interaktiver Aktionsmodus Im interaktiven Aktionsmodus reagieren Sie auf gefundene Viren und unerwünschte Programme, indem Sie in der Warnmeldung eine **Aktion für die betroffenen Objekte** auswählen und die gewählte Aktion durch Bestätigen ausführen.

Folgende Aktionen zur Behandlung betroffener Objekte stehen zur Auswahl:

> **Hinweis**
> Welche Aktionen zur Auswahl stehen, ist abhängig vom Betriebssystem, von der Schutzkomponente (Avira System-Scanner, Avira Echtzeit-Scanner, Avira Email-Schutz, Avira Browser-Schutz), die den Fund meldet und von der gefundenen Malware.

Aktionen des System-Scanners und des Echtzeit-Scanners (ohne Funde von ProActiv):

Reparieren

Die Datei wird repariert.

Diese Option ist nur aktivierbar, wenn eine Reparatur der gefundenen Datei möglich ist.

Umbenennen

Die Datei wird nach **.vir* umbenannt. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurückbenannt werden.

Quarantäne

Die Datei wird in ein spezielles Format (**.qua*) gepackt und in das Quarantäne-Verzeichnis *INFECTED* auf Ihrer Festplatte verschoben, sodass kein direkter Zugriff mehr möglich ist. Dateien in diesem Verzeichnis können später in der Quarantäne repariert oder - falls nötig - an Avira geschickt werden.

Löschen

Die Datei wird gelöscht. Dieser Vorgang ist bedeutend schneller als **Überschreiben und löschen**. Handelt es sich bei dem Fund um einen Bootsektorvirus, wird beim Löschen der Bootsektor gelöscht. Es wird ein neuer Bootsektor geschrieben.

Ignorieren

Es werden keine weiteren Aktionen ausgeführt. Die betroffene Datei bleibt auf Ihrem Computer aktiv.

> **Warnung**
> Gefahr von Datenverlust und Schäden am Betriebssystem! Nutzen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen.

Überschreiben und löschen

Die Datei wird mit einem Standardmuster überschrieben und anschließend gelöscht. Sie kann nicht wiederhergestellt werden.

Immer ignorieren

Aktionsoption bei Funden des Echtzeit-Scanners: Es werden keine weiteren Aktionen vom Echtzeit-Scanner ausgeführt. Ein Zugriff auf die Datei wird zugelassen. Alle weiteren Zugriffe auf diese Datei werden zugelassen und nicht mehr gemeldet bis ein Neustart des Rechners oder ein Update der Virendefinitionsdatei erfolgt.

> **Warnung**
> Gefahr von Datenverlust und Schäden am Betriebssystem! Nutzen Sie die Option **Immer ignorieren** nur in begründeten Ausnahmefällen.

In Quarantäne kopieren

Aktionsoption beim Fund eines Rootkits: Der Fund wird in die Quarantäne kopiert.

Bootsektor reparieren | Repairtool herunterladen

Aktionsoptionen beim Fund von infizierten Bootsektoren: Für infizierte Diskettenlaufwerke stehen Optionen zur Reparatur zur Verfügung. Ist keine Reparatur mit Ihrem Avira Produkt möglich, können Sie ein Spezialtool zum Erkennen und Entfernen von Bootsektorviren herunterladen.

> **Hinweis**
> Wenn Sie Aktionen auf laufende Prozesse anwenden, werden die betroffenen Prozesse vor der Ausführung der Aktion beendet.

Aktionen des Echtzeit-Scanners bei Funden der ProActiv-Komponente (Meldung von verdächtigen Aktionen einer Anwendung):

Vertrauenswürdiges Programm

Die Ausführung der Anwendung wird fortgesetzt. Das Programm wird zur Liste der erlaubten Anwendungen hinzugefügt und von der Überwachung durch die ProActiv-Komponente ausgenommen. Beim Hinzufügen zur Liste der erlaubten Anwendungen wird der Überwachungstyp *Inhalt* gesetzt. Dies bedeutet, dass die Anwendung nur bei unverändertem Inhalt von einer Überwachung durch die ProActiv-Komponente ausgenommen wird (siehe Anwendungsfilter: Auszulassende Anwendungen).

Programm einmal blockieren

Die Anwendung wird blockiert, d.h. die Ausführung der Anwendung wird beendet. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.

Dieses Programm immer blockieren

Die Anwendung wird blockiert, d.h. die Ausführung der Anwendung wird beendet. Das Programm wird zur Liste der zu blockierenden Anwendungen hinzugefügt und kann nicht mehr ausgeführt werden (siehe Anwendungsfilter: Zu blockierende Anwendungen).

Ignorieren

Die Ausführung der Anwendung wird fortgesetzt. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.

Aktionen des Email-Schutzes: Eingehende Emails

In Quarantäne verschieben

Die Email wird inklusive aller Anhänge in Quarantäne verschoben. Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge werden durch einen Standardtext ersetzt.

Email löschen

Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge werden durch einen Standardtext ersetzt.

Anhang löschen

Der betroffene Anhang wird durch einen Standardtext ersetzt. Sollte der Textkörper der Email betroffen sein, wird dieser gelöscht und ebenfalls durch einen Standardtext ersetzt. Die Email selbst wird zugestellt.



Anhang in Quarantäne verschieben

Der betroffene Anhang wird in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Der Textkörper der Email wird zugestellt. Die betroffene Anlage kann später über den Quarantänemanager zugestellt werden.

Ignorieren

Die betroffene Email wird zugestellt.

> **Warnung**
> Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen. Deaktivieren Sie die Vorschau in Microsoft Outlook, starten Sie Anlagen auf keinen Fall per Doppelklick!

Aktionen des Email-Schutzes: Ausgehende Emails

Mail in Quarantäne verschieben (nicht senden)

Die Email wird inklusive aller Anhänge in die Quarantäne kopiert und nicht gesendet. Die Email verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

Mailversand blockieren (nicht senden)

Die Email wird nicht versandt und verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

Ignorieren

Die betroffene Email wird versendet.

> **Warnung**
> Hierdurch können Viren sowie unerwünschte Programme auf das Computersystem des Email-Empfängers gelangen.

Aktionen des Browser-Schutzes:

Zugriff verweigern

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt.

In Quarantäne verschieben

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden in die Quarantäne verschoben. Die betroffene Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Ignorieren

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom Browser-Schutz an Ihren Webbrowser weitergeleitet.

Warnung
Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen.

Hinweis
Wir empfehlen, eine verdächtige Datei, die nicht repariert werden kann, in die Quarantäne zu verschieben.

Hinweis
Schicken Sie uns auch Dateien, die von der Heuristik gemeldet werden, zur Analyse zu.
Sie können diese Dateien z.B. über unsere Webseite hochladen:
http://www.avira.de/sample-upload
Dateien, die von der Heuristik gemeldet werden, erkennen Sie an der Bezeichnung *HEUR/* bzw. *HEURISTIC/*, die dem Dateinamen vorangestellt werden, z.B.: *HEUR/testdatei.**.

4.3.11 Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen

So können Sie mit Dateien in der Quarantäne umgehen:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Quarantäne**.
- Prüfen Sie, um welche Dateien es sich handelt, sodass Sie deren Originale ggf. von anderer Stelle zurück auf Ihren Computer laden können.

Wenn Sie nähere Informationen zu einer Datei ansehen wollen:

- Markieren Sie die Datei und klicken Sie auf *i* .
  - ↳ Das Dialogfenster **Eigenschaften** mit weiteren Informationen zur Datei erscheint.

Wenn Sie eine Datei erneut prüfen wollen:

Die Prüfung einer Datei empfiehlt sich, wenn die Virendefinitionsdatei Ihres Avira Produkts aktualisiert wurde und ein Verdacht auf einen Fehlalarm vorliegt. So können Sie einen Fehlalarm beim erneuten Prüfen bestätigen und die Datei wiederherstellen.

- Markieren Sie die Datei und klicken Sie auf .
  - ↪ Die Datei wird mit den Einstellungen der Direktsuche auf Viren und Malware geprüft.
  - ↪ Nach der Prüfung erscheint der Dialog **Prüfstatistik**, der eine Statistik zum Zustand der Datei vor und nach der erneuten Prüfung anzeigt.

Wenn Sie eine Datei löschen wollen:

- Markieren Sie die Datei und klicken Sie auf .
- Sie müssen Ihre Auswahl mit **Ja** bestätigen.

Wenn Sie die Datei zur Analyse auf einen Webserver des Avira Malware Research Center hochladen möchten:

- Markieren Sie die Datei, die Sie hochladen möchten.
- Klicken Sie auf .
  - ↪ Es öffnet sich der Dialog *Datei-Upload* mit einem Formular zur Eingabe Ihrer Kontaktdaten.
- Geben Sie die Daten vollständig an.
- Wählen Sie einen Typ aus: **Verdächtige Datei** oder **Verdacht auf Fehlalarm**.
- Wählen Sie ein Antwortformat aus: **HTML**, **Text**, **HTML & Text**.
- Klicken Sie **OK.**
  - ↪ Die Datei wird gepackt auf einen Webserver des Avira Malware Research Center hochgeladen.

> **Hinweis**
> In folgenden Fällen wird eine Analyse durch das Avira Malware Research Center empfohlen:
> **Heuristischer Treffer (Verdächtige Datei)**: Bei einem Suchlauf wurde eine Datei von Ihrem Avira Produkt als verdächtig eingestuft und in die Quarantäne verschoben: Im Dialogfenster zum Virenfund oder in der Reportdatei des Suchlaufs wurde die Analyse der Datei durch das Avira Malware Research Center empfohlen.
> **Verdächtige Datei**: Sie halten eine Datei für verdächtig und haben diese deshalb zur Quarantäne hinzugefügt, die Prüfung der Datei auf Viren und Malware ist jedoch negativ.

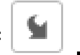


Verdacht auf Fehlalarm: Sie gehen davon aus, dass es sich bei einem Virenfund um einen Fehlalarm handelt: Ihr Avira Produkt meldet einen Fund in einer Datei die jedoch mit hoher Wahrscheinlichkeit nicht von Malware betroffen ist.

Hinweis
Die Größe der Dateien, die Sie hochladen, ist begrenzt auf 20 MB ungepackt oder 8 MB gepackt.

Hinweis
Sie können jeweils nur eine einzelne Datei hochladen.

Wenn Sie die Eigenschaften eines Quarantäne-Objekts in eine Textdatei exportieren möchten:

- Markieren Sie das Quarantäne-Objekt und klicken Sie auf  .
  - ↳ Es öffnet sich eine Textdatei mit den Daten zum ausgewählten Quarantäne-Objekt.
- Speichern Sie die Textdatei ab.

Dateien in Quarantäne können Sie auch wiederherstellen (siehe Kapitel: Quarantäne: Dateien in der Quarantäne wiederherstellen).

4.3.12 Quarantäne: Dateien in der Quarantäne wiederherstellen

Je nach Betriebsystem stehen für das Wiederherstellen verschiedene Symbole zur Verfügung:

- **Unter Windows XP**:

  Mit diesem Symbol stellen Sie Dateien im ursprünglichen Verzeichnis wieder her.
  Mit diesem Symbol stellen Sie Dateien in einem Verzeichnis Ihrer Wahl wieder her.

- **Ab Windows Vista**:

  Ab Microsoft Windows Vista hat das Control Center zunächst nur eingeschränkte Rechte z.B. für den Zugriff auf Verzeichnisse und Dateien. Bestimmte Aktionen und Dateizugriffe kann das Control Center nur mit erweiterten Administratorrechten ausführen. Diese erweiterten Administratorrechte müssen bei jedem Start einer Suche über ein Suchprofil erteilt werden.

Mit diesem Symbol stellen Sie Dateien in einem Verzeichnis Ihrer Wahl wieder her.

Mit diesem Symbol stellen Sie Dateien im ursprünglichen Verzeichnis wieder her. Wenn für den Zugriff auf dieses Verzeichnis erweiterte Administratorrechte nötig sind, erscheint eine entsprechende Abfrage.

So können Sie Dateien in der Quarantäne wiederherstellen:

Warnung
Gefahr von Datenverlust und Schäden am Betriebssystem des Computers!
Verwenden Sie die Funktion **Ausgewähltes Objekt wiederherstellen** nur in Ausnahmefällen. Stellen Sie nur solche Dateien wieder her, die durch einen erneuten Suchlauf repariert werden konnten.

✓ Datei erneut mit Suchlauf geprüft und repariert.

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Quarantäne**.

Hinweis
Emails und Anhänge von Emails können nur mit der Option und mit der Endung **.eml* wiederhergestellt werden.

Wenn Sie eine Datei an ihrem Ursprungsort wiederherstellen wollen:

- Markieren Sie die Datei und klicken Sie auf das Symbol (Windows XP: , ab Windows Vista).

Diese Option ist für Emails nicht möglich.

Hinweis
Emails und Anhänge von Emails können nur mit der Option und mit der Endung **.eml* wiederhergestellt werden.

↳ Eine Abfrage erscheint, ob Sie die Datei wiederherstellen wollen.

- Klicken Sie auf **Ja**.

↳ Die Datei wird in dem Verzeichnis wiederhergestellt, aus dem sie in die Quarantäne verschoben wurde.

Wenn Sie eine Datei in einem bestimmten Verzeichnis wiederherstellen wollen:

- Markieren Sie die Datei und klicken Sie auf .

↳ Eine Abfrage erscheint, ob Sie die Datei wiederherstellen wollen.

- Klicken Sie auf **Ja**.

↳ Das Windows-Standardfenster für die Auswahl des Verzeichnisses erscheint.

- Wählen Sie das Verzeichnis, in dem die Datei wiederhergestellt werden soll und bestätigen Sie.

↳ Die Datei wird in dem gewählten Verzeichnis wiederhergestellt.

4.3.13 Quarantäne: Verdächtige Datei in die Quarantäne verschieben

So können Sie manuell eine verdächtige Datei in die Quarantäne verschieben:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Quarantäne**.
- Klicken Sie auf [+] .

↳ Das Windows-Standardfenster für die Auswahl einer Datei erscheint.

- Wählen Sie die Datei und bestätigen Sie mit **Öffnen**.

↳ Die Datei wird in die Quarantäne verschoben.

Dateien in Quarantäne können Sie mit dem Avira System-Scanner prüfen (siehe Kapitel: Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen).

4.3.14 Suchprofil: Dateityp in einem Suchprofil ergänzen oder löschen

So legen Sie für ein Suchprofil fest, dass zusätzliche Dateitypen durchsucht oder dass bestimmte Dateitypen von der Suche ausgeschlossen werden sollen (nur bei manueller Auswahl und selbstdefinierten Suchprofilen möglich):

✓ Sie befinden sich im Control Center in der Rubrik *PC SICHERHEIT* **> Prüfen**.

- Klicken Sie mit der rechten Maustaste auf das Suchprofil, das Sie bearbeiten wollen.

↳ Ein Kontextmenü erscheint.

- Wählen Sie den Eintrag **Dateifilter**.
- Klappen Sie das Kontextmenü weiter auf, indem Sie auf das kleine Dreieck auf der rechten Seite des Kontextmenüs klicken.

↳ Die Einträge **Standard**, **Prüfe alle Dateien** und **Benutzerdefiniert** erscheinen.

- Wählen Sie den Eintrag **Benutzerdefiniert**.

↳ Das Dialogfenster **Dateierweiterungen** erscheint mit einer Liste aller Dateitypen, die mit dem Suchprofil durchsucht werden.

Wenn Sie einen Dateityp aus der Suche ausschließen wollen:

- Markieren Sie den Dateityp und klicken Sie auf **Löschen**.

Wenn Sie einen Dateityp zur Suche hinzufügen wollen:

- Markieren Sie einen Dateityp.
- Klicken Sie auf **Einfügen** und geben Sie die Dateierweiterung des Dateityps in das Eingabefeld ein.

  Verwenden Sie dabei maximal 10 Zeichen und geben Sie den führenden Punkt nicht mit an. Platzhalter (* und ?) sind erlaubt.

4.3.15 Suchprofil: Desktop-Verknüpfung für Suchprofil erstellen

Über eine Desktop-Verknüpfung zu einem Suchprofil können Sie eine Direktsuche direkt von Ihrem Desktop aus starten, ohne das Control Center Ihres Avira Produktes aufzurufen.

So erstellen Sie eine Verknüpfung zu dem Suchprofil auf dem Desktop:

✓ Sie befinden sich im Control Center in der Rubrik *PC SICHERHEIT* **> Prüfen**.

- Wählen Sie das Suchprofil, zu dem Sie eine Verknüpfung erstellen möchten.
- Klicken Sie auf das Symbol .

  ↳ Die Desktop-Verknüpfung wird erstellt.

4.3.16 Ereignisse: Ereignisse filtern

Im Control Center werden unter *VERWALTUNG* **> Ereignisse** alle Ereignisse angezeigt, die von den Programmkomponenten Ihres Avira Produkts erzeugt wurden (analog der Ereignisanzeige Ihres Windows Betriebssystems). Die Programmkomponenten, in ihrer alphabetischen Reihenfolge, sind die folgenden:

- Hilfsdienst
- Email-Schutz
- Echtzeit-Scanner
- Planer
- System-Scanner
- Updater
- Browser-Schutz
- ProActiv

Es werden folgende Ereignistypen angezeigt:

- *Information*
- *Warnung*
- *Fehler*
- *Fund*

So filtern Sie die angezeigten Ereignisse:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* > Ereignisse.
- Aktivieren Sie die Kontrollkästchen der Programmkomponenten, um die Ereignisse der aktivierten Komponenten anzuzeigen.

  - ODER -

  Deaktivieren Sie die Kontrollkästchen der Programmkomponenten, um die Ereignisse der deaktivierten Komponenten auszublenden.
- Aktivieren Sie die Kontrollkästchen der Ereignistypen, um diese Ereignisse anzuzeigen.

  - ODER -

  Deaktivieren Sie die Kontrollkästchen der Ereignistypen, um diese Ereignisse auszublenden.

4.3.17 Email-Schutz: Email-Adressen von der Prüfung ausschließen

So stellen Sie ein, welche Email-Adressen (Absender) von der Prüfung durch den Email-Schutz ausgeschlossen werden (sogenanntes Whitelisting):

- Wählen Sie im Control Center die Rubrik *INTERNET SICHERHEIT* **> Email-Schutz**.

  ↳ In der Liste sehen Sie die eingegangenen Emails.
- Markieren Sie die Email, die Sie von der Prüfung des Email-Schutzes ausschließen möchten.
- Klicken Sie auf das gewünschte Symbol, um die Email von der Prüfung des Email-Schutzes auszuschließen:

  Die ausgewählte Email-Adresse wird in Zukunft nicht mehr auf Viren und unerwünschte Programme geprüft.

  ↳ Die Email-Absender-Adresse wird in die Ausschlussliste übernommen und nicht mehr auf Viren und Malware geprüft.

Warnung
Schließen Sie nur Email-Adressen von absolut vertrauenswürdigen Absendern von der Prüfung des Email-Schutz aus.

Hinweis
In der Konfiguration unter Email Schutz > Allgemeines > Ausnahmen können Sie weitere Email-Adressen in die Ausschlussliste einpflegen oder Email-Adressen aus der Ausschlussliste entfernen.



5. Fund

5.1 Überblick

Bei Virenfunden kann Ihr Avira Produkt automatisch bestimmte Aktionen ausführen oder interaktiv reagieren. Im interaktiven Aktionsmodus öffnet sich beim Virenfund ein Dialog, in dem Sie die weitere Behandlung des Virus (Löschen, Ignorieren etc.) steuern oder anstoßen. Im automatischen Modus besteht die Option, beim Virenfund eine Warnmeldung anzeigen zu lassen. In der Meldung wird die Aktion, die automatisch ausgeführt wurde, angezeigt.

In diesem Kapitel erhalten Sie, nach Modulen geordnet, alle Informationen über die Meldungen eines Funds.

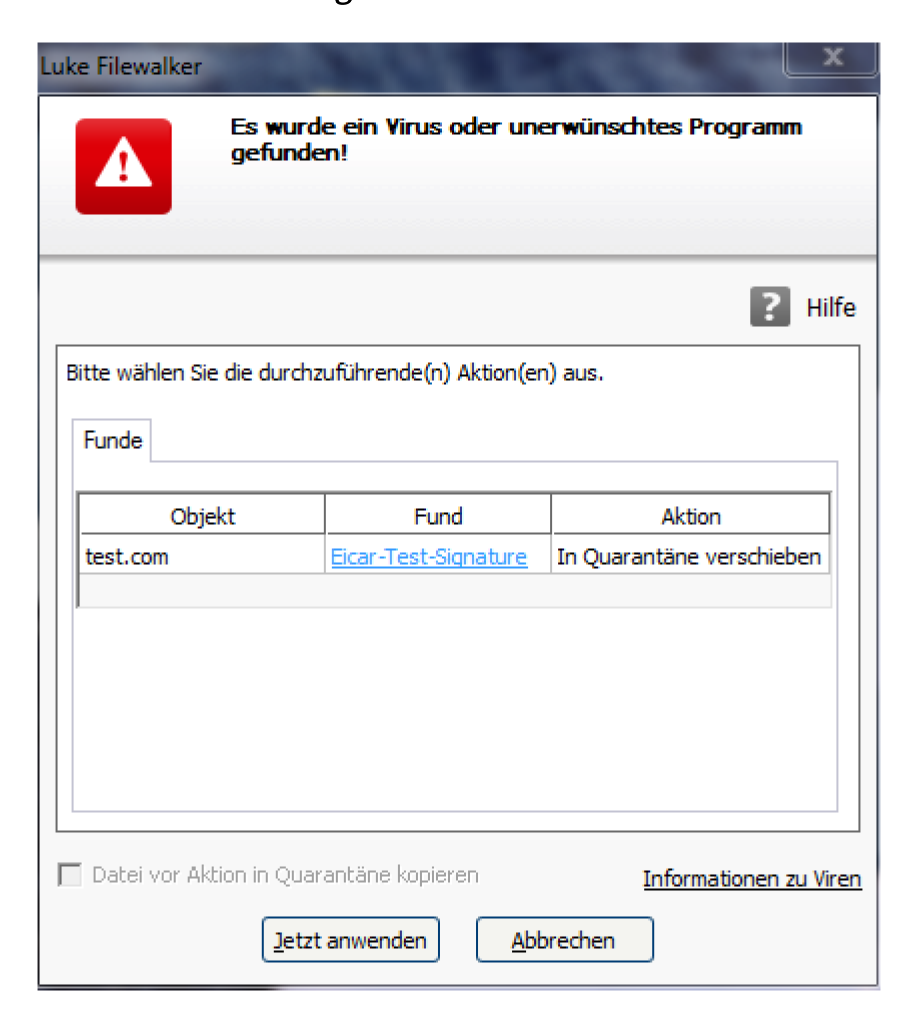
- siehe Kapitel System-Scanner: Interaktiver Aktionsmodus
- siehe Kapitel System Scanner: Dateien an Cloud-Sicherheit senden
- siehe Kapitel Echtzeit-Scanner
- siehe Kapitel Echtzeit Scanner: Verdächtiges Verhalten
- siehe Kapitel Email-Schutz: Eingehende Emails
- siehe Kapitel Email-Schutz: Ausgehende Emails
- siehe Kapitel Browser-Schutz

5.2 Interaktiver Aktionsmodus

Bei der Dateisuche des System-Scanners erhalten Sie beim Abschluss der Suche eine Warnmeldung mit einer Liste der gefundenen betroffenen Dateien, wenn Sie als Aktionsmodus für Virenfunde den Modus *interaktiv* gewählt haben (siehe die Konfigurationsrubrik System-Scanner > Suche > Aktion bei Fund).
Sie haben die Möglichkeit, über das Kontextmenü eine auszuführende Aktion für die einzelnen betroffenen Dateien auszuwählen. Sie können die gewählten Aktionen für alle betroffenen Dateien ausführen oder den System-Scanner beenden.

> **Hinweis**
> Bei aktivierter Protokollierung trägt der System-Scanner jeden Fund in der Reportdatei ein.

5.2.1 Warnmeldung



5.2.2 Fund, Fehler, Warnungen

Unter den Registerkarten **Fund**, **Fehler** und **Warnungen** werden Detailinformationen und Aktionsoptionen zu den Virenfunden sowie Meldungen angezeigt:

- **Fund:**
  - *Objekt:* Dateiname der betroffenen Datei
  - *Fund:* Name des gefundenen Virus bzw. unerwünschten Programms
  - *Aktion:* Ausgewählte Aktion, mit der die betroffene Datei behandelt werden soll
    Im Kontextmenü zur angezeigten Aktion können Sie weitere Aktionen zur Behandlung der Malware auswählen.
- **Fehler:** Meldungen über Fehler, die während des Suchlaufs aufgetreten sind
- **Warnungen:** Warnmeldungen, die sich auf die Virenfunde beziehen

Hinweis
Im Tooltip zum Objekt werden folgende Informationen angezeigt: Name der

betroffenen Datei und vollständiger Pfad, Name des Virus, Aktion die mit der Schaltfläche **Jetzt anwenden** ausgeführt wird.

Hinweis
Als auszuführende Aktion wird standardmäßig die Standardaktion des System-Scanners angezeigt. Die Standardaktion des System-Scanners zur Behandlung von betroffenen Dateien ist das Verschieben der betroffenen Datei in die Quarantäne.

5.2.3 Kontextmenü Aktionen

Hinweis
Handelt es sich bei einem Fund um einen heuristischen Treffer (HEUR/), um einen ungewöhnlichen Laufzeitpacker (PCK/) bzw. eine Datei mit einer verschleierten Dateiendung (HEUR-DBLEXT/), stehen im interaktiven Modus nur die Optionen In Quarantäne verschieben und Ignorieren zur Verfügung. Im automatischen Modus wird der Fund automatisch in die Quarantäne verschoben.
Diese Einschränkung verhindert, dass gefundene Dateien, bei denen es sich eventuell um einen Fehlalarm handelt, direkt von Ihrem Computer entfernt (gelöscht) werden. Die Datei kann mit Hilfe des Quarantänemanagers jederzeit wieder hergestellt werden.

Reparieren

Bei aktivierter Option repariert der System-Scanner die betroffene Datei.

Hinweis
Die Option **Reparieren** ist nur aktivierbar, wenn eine Reparatur der gefundenen Datei möglich ist.

Quarantäne

Bei aktivierter Option verschiebt der System-Scanner die Datei in die Quarantäne. Die Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden. Je nach Datei stehen im Quarantänemanager noch weitere Auswahlmöglichkeiten zur Verfügung.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".



Überschreiben und löschen

Bei aktivierter Option überschreibt der System-Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Umbenennen

Bei aktivierter Option benennt der System-Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Die Datei kann später repariert und zurück benannt werden.

Ignorieren

Bei aktivierter Option wird die Datei belassen.

Immer ignorieren

Aktionsoption bei Funden des Echtzeit-Scanners: Es werden keine weiteren Aktionen vom Echtzeit-Scanner ausgeführt. Ein Zugriff auf die Datei wird zugelassen. Alle weiteren Zugriffe auf diese Datei werden zugelassen und nicht mehr gemeldet bis ein Neustart des Rechners oder ein Update der Virendefinitionsdatei erfolgt.

Warnung
Wenn Sie die Optionen Ignorieren oder **Immer ignorieren** wählen, bleiben die betroffenen Dateien auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

5.2.4 Besonderheiten bei Funden von infizierten Bootsektoren, Rootkits und aktiver Malware

Beim Fund von infizierten Bootsektoren stehen Aktionsoptionen für die Reparatur der Bootsektoren zur Verfügung:

722 KB | 1,44 MB | 2,88 MB | 360 KB | 1,2 MB Bootsektor reparieren

Diese Optionen stehen für Diskettenlaufwerke zur Verfügung.

Rescue-CD herunterladen

Über diese Option gelangen Sie zur Avira Webseite, wo Sie ein spezielles Werkzeug zum Erkennen und Entfernen von Bootsektorviren herunterladen können.

Wenn Sie Aktionen auf laufende Prozesse anwenden, werden die betroffenen Prozesse vor der Ausführung der Aktion beendet.

5.2.5 Schaltflächen und Links

Schaltfläche/Link	Description
Jetzt anwenden	Die ausgewählten Aktionen werden zur Behandlung aller betroffenen Dateien ausgeführt.
Abbrechen	Der System-Scanner wird ohne weitere Aktion beendet. Die betroffenen Dateien werden auf Ihrem Computersystem belassen.
Hilfe	Über diese Schaltfläche bzw. den Link wird diese Seite der Online-Hilfe geöffnet.

Warnung
Führen Sie die Aktion *Abbrechen* nur in begründeten Ausnahmefällen durch. Beim Abbrechen bleiben die betroffenen Dateien auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

5.2.6 Besonderheiten bei Funden bei deaktiviertem Browser-Schutz

Sollten Sie den Browser-Schutz deaktiviert haben, meldet der Echtzeit-Scanner gefundene, aktive Malware durch ein Slide-Up während das System überprüft wird. Sie haben die Möglichkeit vor einer Reparatur einen Systemwiederherstellungspunkt zu erzeugen.

✓ Die Funktion der Systemwiederherstellung muss in Ihrem Windows-Betriebssystem aktiviert sein.

- Klicken Sie **Details anzeigen** im Slide-Up.
  - ↳ Das Fenster *System wird geprüft* öffnet sich.
- Aktivieren Sie **Systemwiederherstellungspunkt vor Reparatur erzeugen**.
- Klicken Sie auf die Schaltfläche **Übernehmen**.
  - ↳ Es wurde ein Systemwiederherstellungspunkt erzeugt. Nun können Sie gegebenenfalls über Ihr Windows-Betriebssystem eine Systemwiederherstellung auslösen.

5.3 Dateien an Cloud-Sicherheit senden

Es wird bei jeder **Schnellen Systemprüfung** eine Liste von Dateispeicherorten erstellt, auf welche Malware-Programme abzielen. In dieser Liste sind zum Beispiel laufende

Prozesse, Start- und Dienstprogramme enthalten. Unbekannte Programmdateien werden zur Analyse in das Avira Cloud-Sicherheitssystem hochgeladen.

Wenn Sie während der benutzerdefinierten Installation oder in der Konfiguration des **Erweiterten Schutz** die Option **Manuell bestätigen, wenn verdächtige Dateien an Avira gesendet werden** aktiviert haben, können Sie die Liste der verdächtigen Dateien prüfen und selber auswählen, welche Dateien Sie zur Cloud-Sicherheit hochladen möchten. Standardmäßig werden alle verdächtigen Dateien zum Hochladen zur Avira Cloud-Sicherheit markiert.

> **Hinweis**
> Wenn Sie die **Erweiterte** Protokollierung bei der Konfiguration des System-Scanners aktiviert haben, zeigt die Reportdatei das *(Cloud)*-Suffix an, um die Warnungen von der Cloud-Sicherheit zu identifizieren.

5.3.1 Angezeigte Informationen

Die Liste der verdächtigen Dateien, die zur Avira Cloud-Sicherheit hochgeladen werden sollen.

- *Senden:* Sie können auswählen, welche Dateien Sie zur Avira Cloud-Sicherheit hochladen möchten.
- *Datei:* Dateiname der verdächtigen Datei.
- *Pfad:* Pfad der verdächtigen Datei.

Dateien immer automatisch senden

Solange diese Option aktiv bleibt, werden nach jeder **Schnellen Systemprüfung** die verdächtigen Dateien automatisch, ohne manuelle Bestätigung, zur Analyse an die Cloud-Sicherheit gesendet.

5.3.2 Schaltflächen und Links

Schaltfläche/Link	Beschreibung
Senden	Die ausgewählten Dateien werden zur Avira Cloud-Sicherheit gesendet.
Abbrechen	Der System-Scanner wird ohne weitere Aktion beendet. Die betroffenen Dateien werden auf Ihrem System belassen.



Hilfe	Diese Seite der Online-Hilfe wird geöffnet.
Was ist Cloud-Sicherheit?	Die Web-Seite mit Informationen über Avira Cloud-Sicherheit wird geöffnet.

Verwandte Themen:

- Konfiguration des Erweiterten Schutz
- Benutzerdefinierte Installation
- Report-Konfiguration
- Berichte-Ansicht

5.4 Echtzeit-Scanner

Bei Virenfunden des Echtzeit-Scanners wird der Dateizugriff verweigert und eine Desktop-Benachrichtigung angezeigt, wenn Sie als Aktionsmodus für Virenfunde den Modus *interaktiv* gewählt haben (siehe die Konfigurationsrubrik Echtzeit Scanner > Suche > Aktion bei Fund).

Benachrichtigung

In der Benachrichtigung werden folgende Informationen angezeigt:

- Datum und Uhrzeit des Funds
- Pfad und Name der betroffenen Datei
- Name der Malware

> **Hinweis**
> Die Auswahl des standardmäßigen Startmodus für den Echtzeit-Scanner (Normaler Start) und ein schnelles Anmelden des Benutzerkontos hat beim Start des Rechners u. U. zur Folge, dass die bei Systemstart automatisch startenden Programmen nicht gescannt werden, da diese noch vor dem vollständigen Laden des Echtzeit-Scanners gestartet worden sind.

Im interaktiven Modus haben Sie folgende Optionen:

Entfernen

Die betroffene Datei wird an die Komponente **System-Scanner** übergeben und vom System Scanner gelöscht. Es erscheint keine weitere Meldung.



Details

Die betroffene Datei wird an die Komponente **System-Scanner** übergeben. Der System-Scanner meldet den Fund in einem Fenster, in dem Sie verschiedene Optionen zur Behandlung der betroffenen Datei haben.

Hinweis
Beachten Sie die Hinweise zur Virenbehandlung unter Fund > System-Scanner.

Hinweis
Standardmäßig ist in der Meldung des System-Scanner die Aktion *Quarantäne* vorausgewählt. Über ein Kontextmenü können Sie weitere Aktionen auswählen.

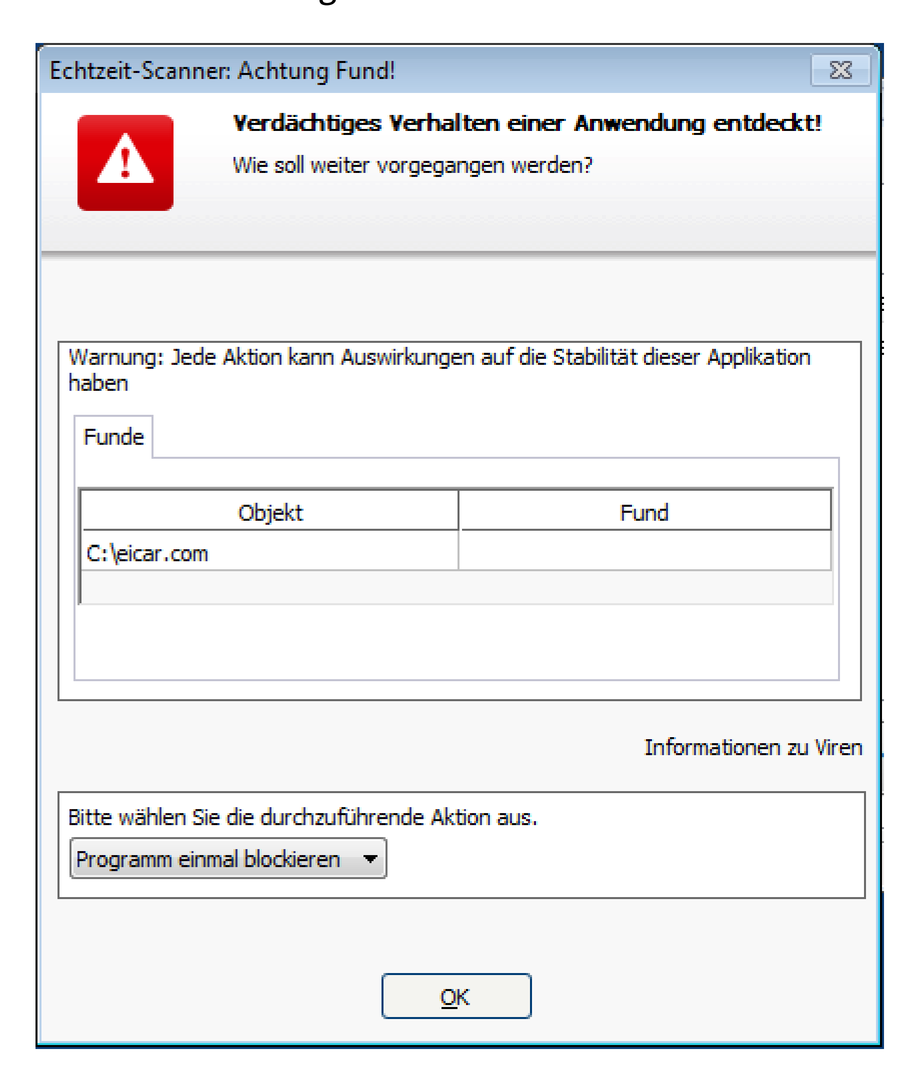
Schließen

Die Meldung wird geschlossen. Die Virenbehandlung wird abgebrochen.

5.5 Verdächtiges Verhalten

Wenn Sie die ProActiv-Komponente des Echtzeit-Scanners aktivieren, werden Aktionen von Anwendungen überwacht und auf ein verdächtiges Verhalten, das für Malware typisch ist, überprüft. Tritt ein verdächtiges Verhalten einer Anwendung auf, erhalten Sie eine Warnmeldung. Sie haben verschiedene Optionen auf den Fund zu reagieren.

5.5.1 Warnmeldung des Echtzeit-Scanners: Verdächtiges Verhalten einer Anwendung entdeckt



5.5.2 Name und Pfad des aktuell gefundenen, verdächtigen Programms

Im mittleren Fenster der Meldung wird der Name und Pfad der Anwendung angezeigt, die verdächtige Aktionen ausführt.

5.5.3 Auswahlmöglichkeiten

Vertrauenswürdiges Programm

Bei aktivierter Option wird die Ausführung der Anwendung fortgesetzt. Das Programm wird zur Liste der erlaubten Anwendungen hinzugefügt und von der Überwachung durch die ProActiv-Komponente ausgenommen. Beim Hinzufügen zur Liste der erlaubten Anwendungen wird der Überwachungstyp *Inhalt* gesetzt. Dies bedeutet, dass die Anwendung nur bei unverändertem Inhalt von einer Überwachung durch die ProActiv-Komponente ausgenommen wird (siehe Anwendungsfilter: Erlaubte Anwendungen).



Programm einmal blockieren

Bei aktivierter Option wird die Anwendung blockiert, d.h. die Ausführung der Anwendung wird beendet. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.

Dieses Programm immer blockieren

Bei aktivierter Option wird die Anwendung blockiert, d.h. die Ausführung der Anwendung wird beendet. Das Programm wird zur Liste der zu blockierenden Anwendungen hinzugefügt und kann nicht mehr ausgeführt werden (siehe Anwendungsfilter: Zu blockierende Anwendungen).

Ignorieren

Bei aktivierter Option wird die Ausführung der Anwendung fortgesetzt. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.

5.5.4 Schaltflächen und Links

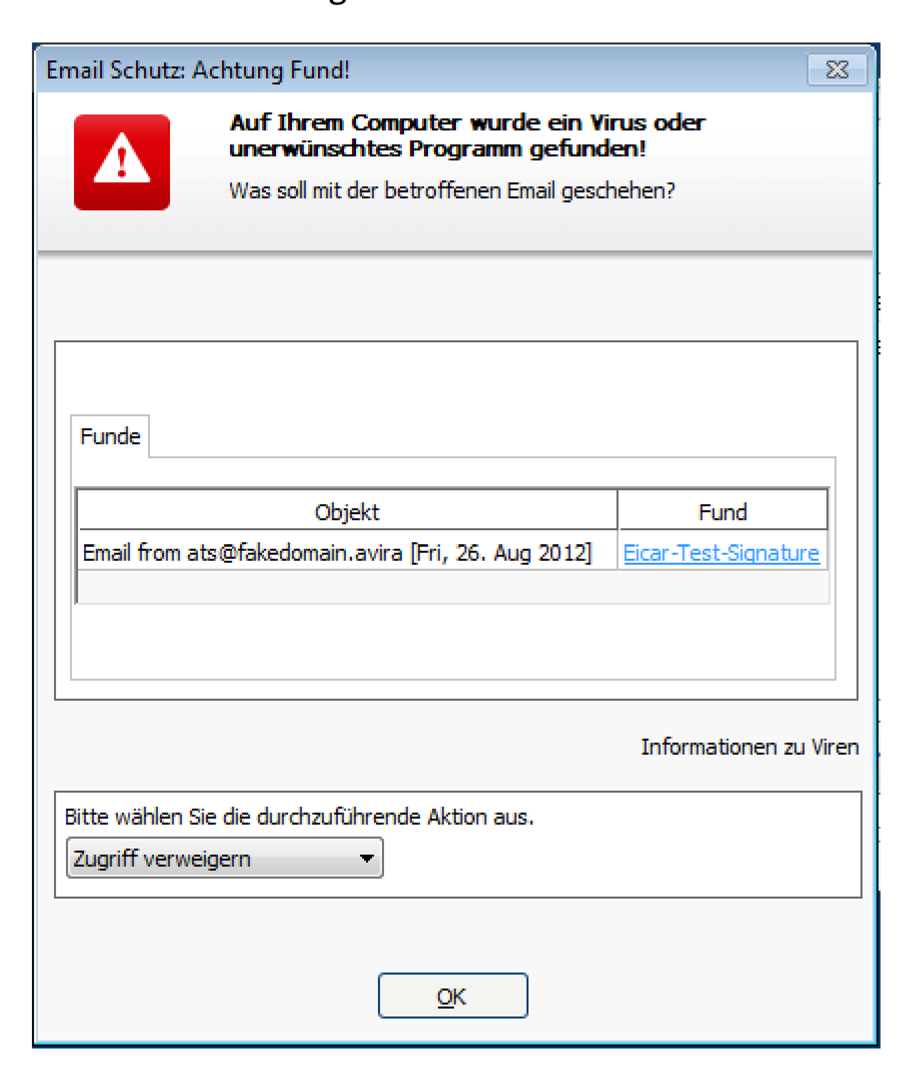
Schaltfläche / Link	Beschreibung
Informationen zu Viren	Über diesen Link gelangen Sie - bei aktiver Internetverbindung - auf eine Internetseite mit weiteren Informationen zu diesem Virus bzw. unerwünschten Programm.
Hilfe	Über diese Schaltfläche bzw. den Link wird diese Seite der Online-Hilfe geöffnet.

5.6 Eingehende Emails

Bei Virenfunden des Email-Schutzes erhalten Sie eine Warnmeldung, wenn Sie als Aktionsmodus für Virenfunde den Modus *interaktiv* gewählt haben (siehe die Konfigurationsrubrik Email Schutz > Suche > Aktion bei Fund). Im interaktiven Modus können Sie in dem Dialogfenster auswählen, was mit der Email oder der Anlage geschehen soll.

Die unten abgebildete Warnmeldung erhalten Sie beim Virenfund in einer eingehenden Email.

5.6.1 Warnmeldung



5.6.2 Funde, Fehler, Warnungen

Unter den Registerkarten **Funde**, **Fehler** und **Warnungen** werden Meldungen und Detailinformationen zu den betroffenen Emails angezeigt:

- **Funde:** Objekt: Betroffene Email mit Angabe des Absenders und des Zeitpunkts, an dem die Email gesendet wurde

  Fund: Name des gefundenen Virus bzw. unerwünschten Programms
- **Fehler:** Meldungen über Fehler, die während der Prüfung durch den Email-Schutz aufgetreten sind
- **Warnungen:** Warnmeldungen, die sich auf die betroffenen Objekte beziehen



5.6.3 Auswahlmöglichkeiten

Hinweis
Handelt es sich bei einem Fund um einen heuristischen Treffer (HEUR/), um einen ungewöhnlichen Laufzeitpacker (PCK/) bzw. eine Datei mit einer verschleierten Dateiendung (HEUR-DBLEXT/), stehen im interaktiven Modus nur die Optionen In Quarantäne verschieben und Ignorieren zur Verfügung. Im automatischen Modus wird der Fund automatisch in die Quarantäne verschoben.
Diese Einschränkung verhindert, dass gefundene Dateien, bei denen es sich eventuell um einen Fehlalarm handelt, direkt von Ihrem Computer entfernt (gelöscht) werden. Die Datei kann mit Hilfe des Quarantänemanagers jederzeit wieder hergestellt werden.

In Quarantäne verschieben

Bei aktivierter Option wird die Email inklusive aller Anhänge in Quarantäne verschoben. Sie kann später über den Quarantänemanager zugestellt werden. Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge der Email werden durch einen Standardtext ersetzt.

Mail löschen

Bei aktivierter Option wird die betroffene Email beim Fund eines Virus bzw. unerwünschten Programms gelöscht. Textkörper und ggf. Anhänge werden durch einen Standardtext ersetzt.

Anhang löschen

Bei aktivierter Option wird der betroffene Anhang durch einen Standardtext ersetzt. Sollte der Textkörper der Email betroffen sein, wird dieser gelöscht und ebenfalls durch einen Standardtext ersetzt. Die Email selbst wird zugestellt.

Anhang in Quarantäne verschieben

Bei aktivierter Option wird der betroffene Anhang in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Der Textkörper der Email wird zugestellt. Die betroffene Anlage kann später über den Quarantänemanager zugestellt werden.

Ignorieren

Bei aktivierter Option wird eine betroffene Email trotz des Funds eines Virus oder unerwünschten Programms zugestellt.

Warnung
Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in



begründeten Ausnahmefällen. Deaktivieren Sie die Vorschau in Microsoft Outlook, starten Sie Anlagen auf keinen Fall per Doppelklick!

5.6.4 Schaltflächen und Links

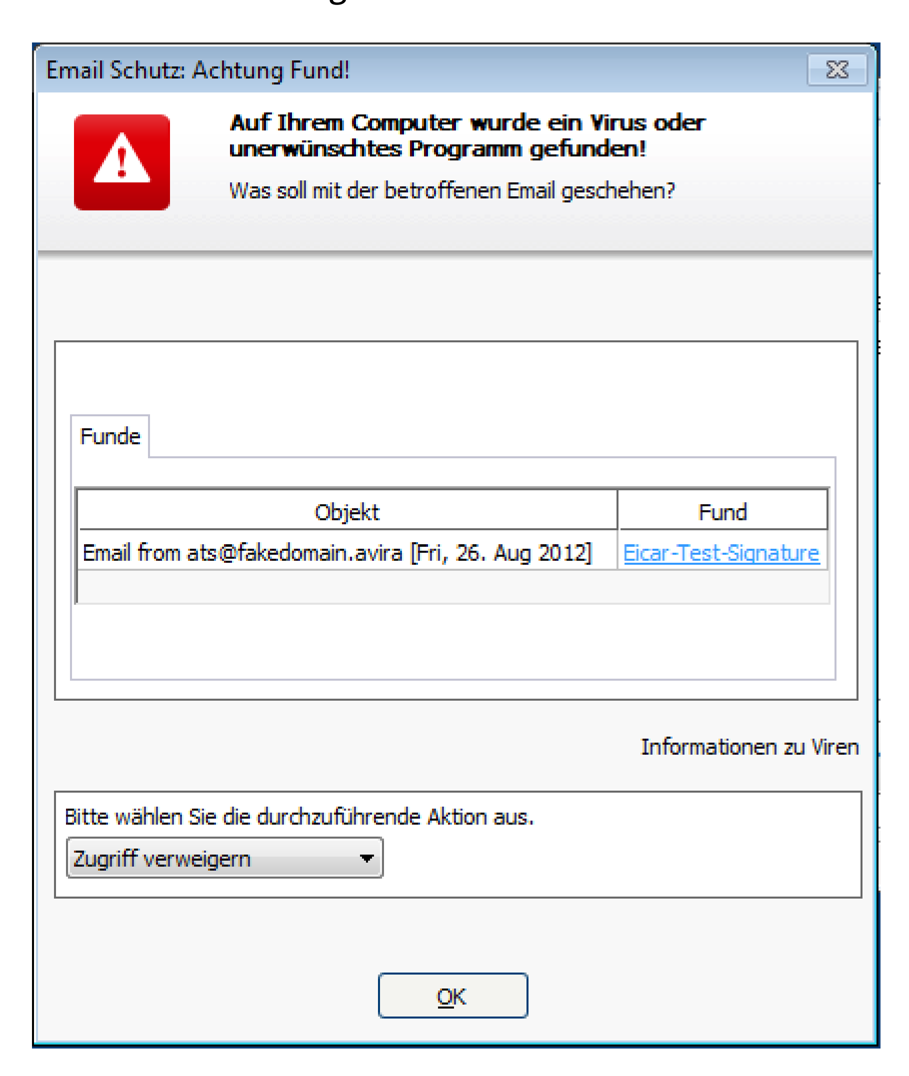
Schaltfläche / Link	Beschreibung
Informationen zu Viren	Über diesen Link gelangen Sie - bei aktiver Internetverbindung - auf eine Internetseite mit weiteren Informationen zu diesem Virus bzw. unerwünschten Programm.
Hilfe	Über diese Schaltfläche bzw. den Link wird diese Seite der Online-Hilfe geöffnet.

5.7 Ausgehende Emails

Bei Virenfunden des Email-Schutzes erhalten Sie eine Warnmeldung, wenn Sie als Aktionsmodus für Virenfunde den Modus *interaktiv* gewählt haben (siehe die Konfigurationsrubrik Email Schutz > Suche > Aktion bei Fund). Im interaktiven Modus können Sie in dem Dialogfenster auswählen, was mit der Email oder der Anlage geschehen soll.



5.7.1 Warnmeldung



5.7.2 Funde, Fehler, Warnungen

Unter den Registerkarten **Funde**, **Fehler** und **Warnungen** werden Meldungen und Detailinformationen zu den betroffenen Emails angezeigt:

- **Funde:** Objekt: Betroffene Email mit Angabe des Absenders und des Zeitpunkts, an dem die Email gesendet wurde

  Fund: Name des gefundenen Virus bzw. unerwünschten Programms

- **Fehler:** Meldungen über Fehler, die während der Prüfung durch den Email-Schutz aufgetreten sind
- **Warnungen:** Warnmeldungen, die sich auf die betroffenen Objekte beziehen



5.7.3 Auswahlmöglichkeiten

Mail in Quarantäne verschieben (nicht senden)

Bei aktivierter Option wird die Email inklusive aller Anhänge in die Quarantäne kopiert und nicht gesendet. Die Email verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

Mailversand blockieren (nicht senden)

Die Email wird nicht versandt und verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

Ignorieren

Bei aktivierter Option wird die betroffene Email trotz des Funds eines Virus oder unerwünschten Programms versendet.

Warnung
Hierdurch können Viren sowie unerwünschte Programme auf das Computersystem des Email-Empfängers gelangen.

5.7.4 Schaltflächen und Links

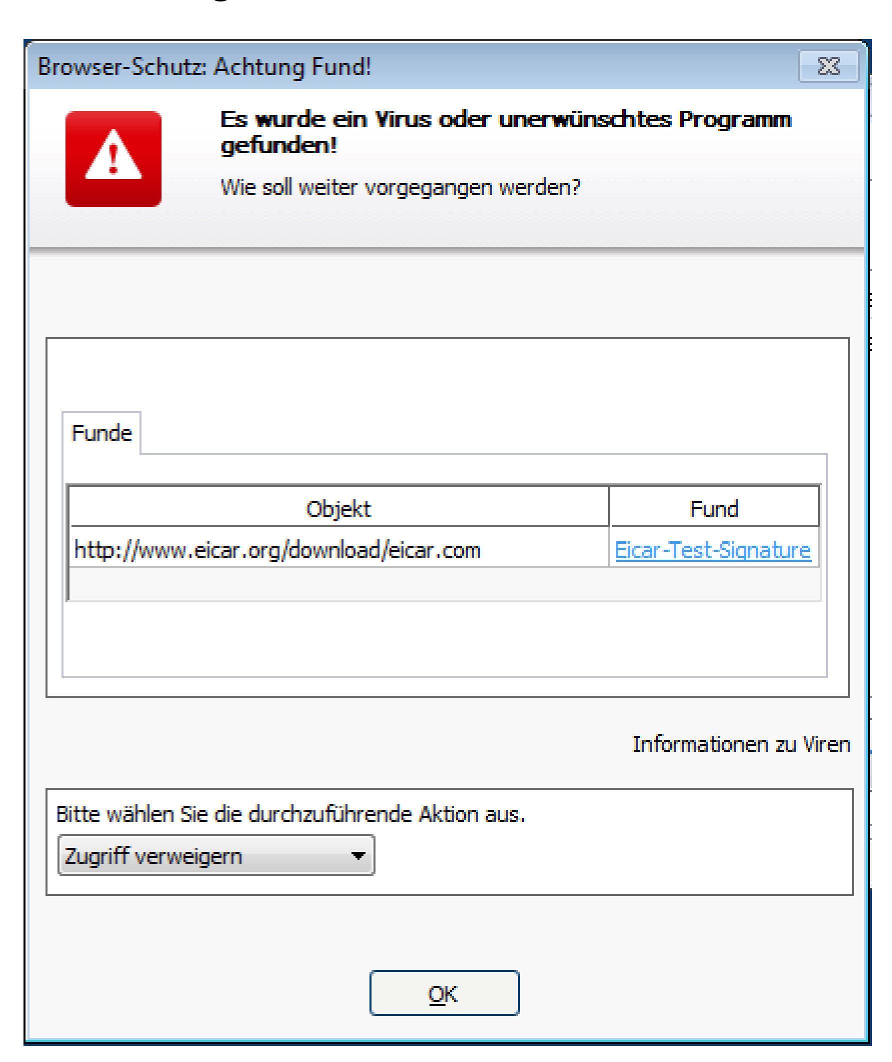
Schaltfläche / Link	Beschreibung
Informationen zu Viren	Über diesen Link gelangen Sie - bei aktiver Internetverbindung - auf eine Internetseite mit weiteren Informationen zu diesem Virus bzw. unerwünschten Programm.
Hilfe	Über diese Schaltfläche bzw. den Link wird diese Seite der Online-Hilfe geöffnet.

5.8 Browser-Schutz

Bei Virenfunden des Browser-Schutzes erhalten Sie eine Warnmeldung, wenn Sie als Aktionsmodus für Virenfunde den Modus *interaktiv* gewählt haben (siehe die Konfigurationsrubrik Browser Schutz > Suche > Aktion bei Fund). Im interaktiven Modus

können Sie in dem Dialogfenster auswählen, was mit den vom Webserver übertragenen Daten geschehen soll.

Warnmeldung



Fund, Fehler, Warnungen

Unter den Registerkarten **Fund**, **Fehler** und **Warnungen** werden Meldungen und Detailinformationen zu den Virenfunden angezeigt:

- **Fund:** URL sowie der Name des gefundenen Virus bzw. unerwünschten Programms
- **Fehler:** Meldungen über Fehler, die während der Prüfung durch den Browser-Schutz aufgetreten sind
- **Warnungen:** Warnmeldungen, die sich auf die Virenfunde beziehen

Mögliche Aktionen

> **Hinweis**
> Handelt es sich bei einem Fund um einen heuristischen Treffer (HEUR/), um

einen ungewöhnlichen Laufzeitpacker (PCK/) bzw. eine Datei mit einer verschleierten Dateiendung (HEUR-DBLEXT/), stehen im interaktiven Modus nur die Optionen In Quarantäne verschieben und Ignorieren zur Verfügung. Diese Einschränkung verhindert, dass gefundene Dateien, bei denen es sich eventuell um einen Fehlalarm handelt, direkt von Ihrem Computer entfernt (gelöscht) werden. Die Datei kann mit Hilfe des Quarantänemanagers jederzeit wieder hergestellt werden.

Zugriff verweigern

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt. Der Browser-Schutz trägt den Fund in die Reportdatei ein, vorausgesetzt die Reportfunktion ist aktiviert.

Isolieren (In Quarantäne verschieben)

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden beim Fund eines Virus bzw. einer Malware in die Quarantäne verschoben. Die betroffene Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Ignorieren

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom Browser-Schutz an Ihren Webbrowser weitergeleitet.

Warnung
Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen.

Schaltflächen und Links

Schaltfläche / Link	Beschreibung
Informationen zu Viren	Über diesen Link gelangen Sie - bei aktiver Internetverbindung - auf eine Internetseite mit weiteren Informationen zu diesem Virus bzw. unerwünschten Programm.
Hilfe	Über diese Schaltfläche bzw. den Link wird diese Seite der Online-Hilfe geöffnet.



6. System-Scanner

6.1 System-Scanner

Mit der Komponente System-Scanner können Sie gezielte Suchläufe nach Viren und unerwünschten Programmen (Direktsuche) ausführen. Sie haben folgende Möglichkeiten nach betroffenen Dateien zu suchen:

- **Direktsuche über Kontextmenü**
  Die Direktsuche über das Kontextmenü (rechte Maustaste - Eintrag **Ausgewählte Dateien mit Avira überprüfen**) empfiehlt sich, wenn Sie z.B. im Windows Explorer einzelne Dateien und Verzeichnisse prüfen wollen. Ein weiterer Vorteil ist, dass für die Direktsuche über das Kontextmenü das Control Center nicht erst gestartet werden muss.
- **Direktsuche über Drag & Drop**
  Beim Ziehen einer Datei oder eines Verzeichnisses in das Programmfenster des Control Center prüft der System-Scanner die Datei bzw. das Verzeichnis sowie alle enthaltenen Unterverzeichnisse. Dieses Vorgehen empfiehlt sich, wenn Sie einzelne Dateien und Verzeichnisse prüfen wollen, die Sie z.B. auf Ihrem Desktop abgelegt haben.
- **Direktsuche über Profile**
  Dieses Vorgehen empfiehlt sich, wenn Sie regelmäßig bestimmte Verzeichnisse und Laufwerke (z.B. Ihr Arbeitsverzeichnis oder Laufwerke, auf denen Sie regelmäßig neue Dateien ablegen) prüfen wollen. Sie müssen diese Verzeichnisse und Laufwerke dann nicht für jede Prüfung neu wählen, sondern wählen eine Auswahl bequem mit dem entsprechenden Profil.
- **Direktsuche über den Planer**
  Der Planer bietet die Möglichkeit, zeitlich gesteuerte Prüfaufträge durchführen zu lassen.

Bei der Suche nach Rootkits, Bootsektorviren und beim Durchsuchen von aktiven Prozessen sind besondere Verfahren erforderlich. Sie haben folgende Optionen:

- Suche nach Rootkits über das Suchprofil *Suche nach Rootkits und aktiver Malware*
- Durchsuchen von aktiven Prozessen über das Suchprofil *Aktive Prozesse*
- Suche nach Bootsektorviren über den Menübefehl **Bootsektorviren prüfen...** im Menü **Extras**

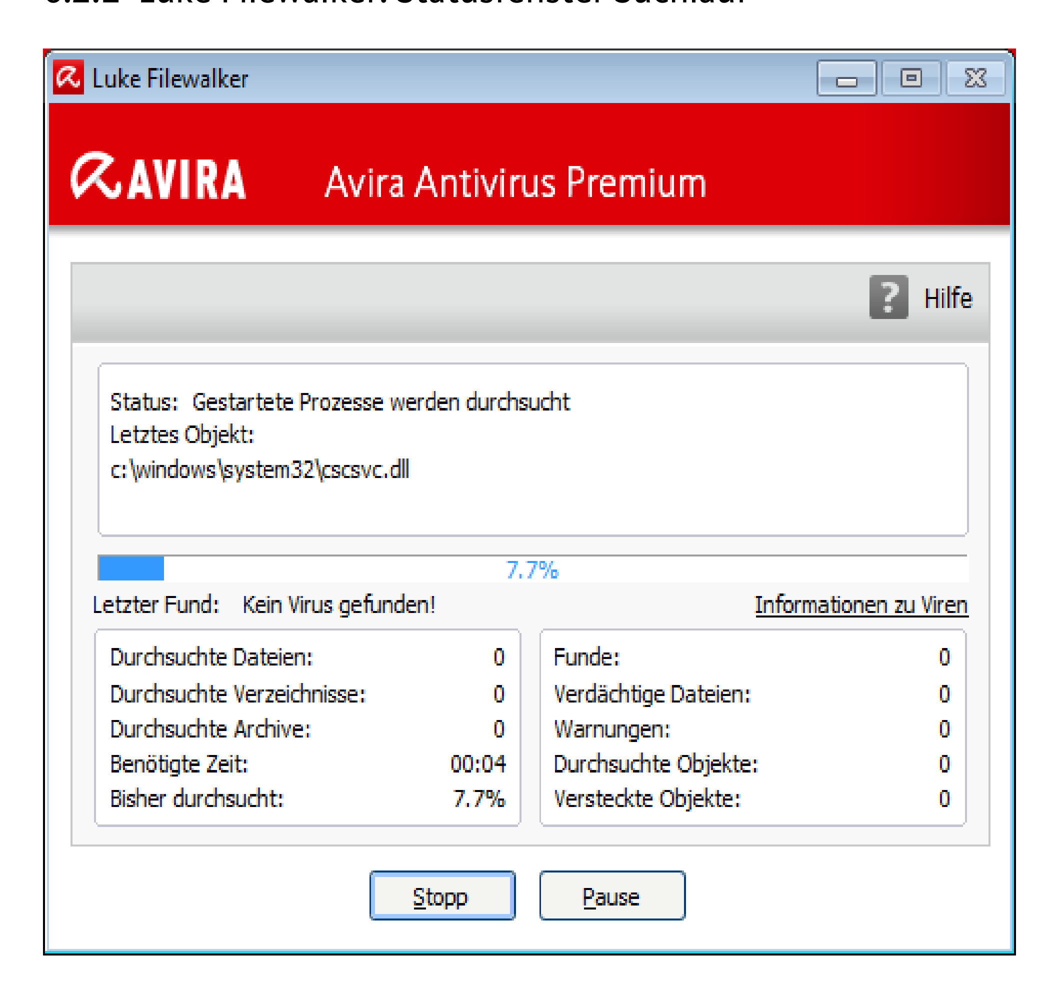
6.2 Luke Filewalker

Während der Direktsuche erscheint das Statusfenster **Luke Filewalker**, das Sie genau über den Stand der Prüfung informiert.

Ist in der Konfiguration des System Scanners in der Gruppe **Aktion bei Fund** die Option **interaktiv** ausgewählt, werden Sie beim Fund eines Virus oder unerwünschten Programms gefragt, was mit diesem geschehen soll. Ist die Option **automatisch** ausgewählt, sind etwaige Funde im Report des System-Scanners sichtbar.

Nach abgeschlossener Suche werden die Ergebnisse des Suchlaufs (Statistik) sowie Fehler- und Warnmeldungen in einem weiteren Dialogfenster angezeigt.

6.2.1 Luke Filewalker: Statusfenster Suchlauf



Angezeigte Informationen

Status: Es gibt unterschiedliche Status-Meldungen:

- *Programm wird initialisiert*
- *Es wird nach versteckten Objekten gesucht!*
- *Gestartete Prozesse werden durchsucht*
- *Die Datei wird durchsucht*
- *Initialisiere Archiv*
- *Speicher freigeben*
- *Datei wird entpackt*

- *Bootsektoren werden durchsucht*
- *Masterbootsektoren werden durchsucht*
- *Die Registry wird durchsucht*
- *Das Programm wird beendet!*
- *Der Suchlauf wurde beendet*

Letztes Objekt: Name und Pfad der Datei, die gerade geprüft wird bzw. zuletzt geprüft wurde

Letzter Fund: Es gibt unterschiedliche Meldungen zum letzten Fund:

- *Kein Virus gefunden!*
- Name des zuletzt gefundenen Virus oder unerwünschten Programms

Durchsuchte Dateien: Anzahl der geprüften Dateien

Durchsuchte Verzeichnisse: Anzahl der geprüften Verzeichnisse

Durchsuchte Archive: Anzahl der geprüften Archive

Benötigte Zeit: Dauer der Direktsuche

Bisher durchsucht: Prozentualer Anteil der bereits durchgeführten Suche

Funde: Anzahl der gefundenen Viren und unerwünschten Programme

Verdächtige Dateien: Anzahl der Dateien, die von der Heuristik gemeldet wurden

Warnungen: Anzahl von Warnmeldungen zu Virenfunden

Durchsuchte Objekte: Anzahl der Objekte, die bei der Rootkits-Suche durchsucht wurden

Versteckte Objekte: Anzahl der insgesamt gefundenen versteckten Objekte

Hinweis
Rootkits haben die Eigenschaft, Prozesse und Objekte wie z.B. Registry-Einträge oder Dateien zu verstecken, jedoch ist nicht jedes verborgene Objekt ein zwingender Hinweis auf die Existenz eines Rootkits. Bei versteckten Objekten kann es sich auch um unschädliche Objekte handeln. Falls beim Suchlauf versteckte Objekte gefunden wurden und keine Warnmeldungen zu Virenfunden vorliegen, sollten Sie anhand des Reports ermitteln, um welche Objekte es sich handelt und weitere Informationen über die gefundenen Objekte einholen.

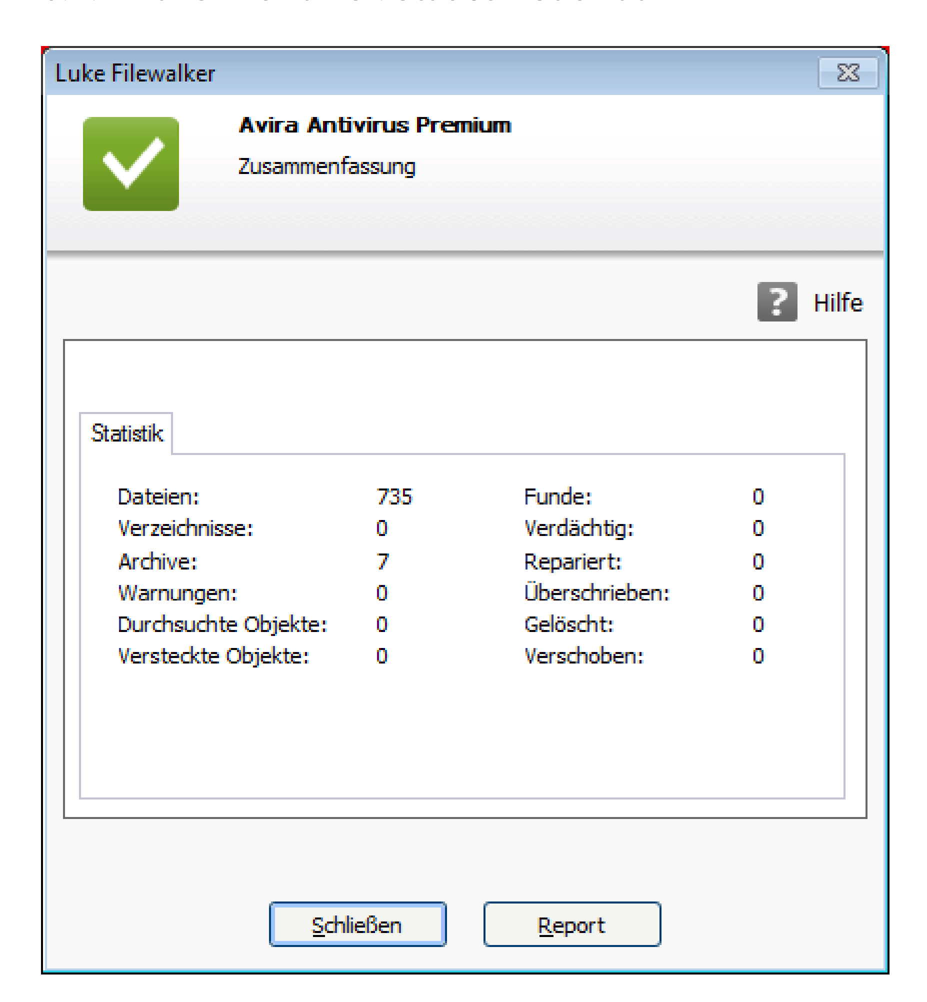
Schaltflächen und Links

Schaltfläche / Link	Beschreibung
Informationen zu Viren	Über diesen Link gelangen Sie - bei aktiver Internetverbindung - auf eine Internetseite mit weiteren Informationen zu diesem Virus bzw. unerwünschten Programm.
Hilfe	Über diese Schaltfläche bzw. den Link wird diese Seite der Online-Hilfe geöffnet.
Stopp	Der Suchvorgang wird gestoppt.
Pause	Der Suchvorgang wird unterbrochen und kann über die Schaltfläche **Fortsetzen** weiter geführt werden.
Fortsetzen	Der unterbrochene Suchvorgang wird fortgesetzt.
Beenden	Der System-Scanner wird geschlossen.



Report	Die Reportdatei des Suchlaufs wird angezeigt.

6.2.2 Luke Filewalker: Statistik Suchlauf



Angezeigte Informationen: Statistik

Dateien: Anzahl der durchsuchten Dateien

Verzeichnisse: Anzahl der durchsuchten Verzeichnisse

Archive: Anzahl der geprüften Archive

Warnungen: Anzahl von Warnmeldungen zu Virenfunden

Durchsuchte Objekte: Anzahl der Objekte, die bei der Rootkits-Suche durchsucht wurden

Versteckte Objekte: Anzahl gefundener versteckter Objekte (Rootkits)

Funde: Anzahl der gefundenen Viren und unerwünschten Programme

Verdächtig: Anzahl der Dateien, die von der Heuristik gemeldet wurden

Repariert: Anzahl reparierter Dateien

Überschrieben: Anzahl überschriebener Dateien

Gelöscht: Anzahl gelöschter Dateien

Verschoben: Anzahl der in Quarantäne verschobenen Dateien

Schaltflächen und Links

Schaltfläche / Link	Beschreibung
Hilfe	Diese Seite der Online-Hilfe geöffnet.
Schließen	Das Fenster der Zusammenfassung wird geschlossen.
Report	Die Reportdatei des Suchlaufs wird angezeigt.

7. Control Center

7.1 Überblick

Das Control Center dient als zentrale Informations-, Konfigurations- und Verwaltungsstelle. Zusätzlich zu den einzeln auswählbaren Rubriken bietet es eine Vielzahl an Optionen, die über die Menüleiste anwählbar sind.

Menüleiste

In der Menüleiste finden Sie folgende Funktionen:

Datei

- Beenden (Alt+F4)

Ansicht

- Status
- PC Sicherheit
  - System-Scanner
  - Echtzeit-Scanner
- Internet Sicherheit
  - FireWall
  - Browser-Schutz
  - E-Mail-Schutz
- Kinderschutz
  - Soziale Netzwerke
- Mobiler Schutz
  - Avira Android Security
- Verwaltung
  - Quarantäne
  - Planer
  - Berichte
  - Ereignisse
- Aktualisieren (F5)

Extras

- Bootsektoren prüfen...

- Erkennungsliste...
- Rescue-CD herunterladen
- Konfiguration (F8)

Update

- Update starten...
- Manuelles Update...

Hilfe

- Inhalte
- Hilf mir
- Live Support
- Forum
- Download Handbuch
- Lizenzmanagement
- Produkt empfehlen
- Feedback senden
- Über Avira Antivirus Suite

> **Hinweis**
> Die Tastaturnavigation in der Menüleiste aktivieren Sie mit Hilfe der [Alt]-Taste. Ist die Navigation aktiviert, können Sie sich mit den Pfeiltasten innerhalb des Menüs bewegen. Mit der Return-Taste aktivieren Sie den aktuell markierten Menüpunkt.

Rubriken

In der linken Navigationsleiste finden Sie folgende Rubriken:

- **Status**

PC SICHERHEIT

- System-Scanner
- Echtzeit-Scanner

INTERNET SICHERHEIT

- FireWall
- Browser-Schutz
- Email-Schutz

KINDERSCHUTZ

- Soziale Netzwerke

MOBILER SCHUTZ

- Avira Android Security

VERWALTUNG

- Quarantäne
- Planer
- Berichte
- Ereignisse

Rubriken-Beschreibung

- **Status**: Im Startbildschirm **Status** finden Sie alle Rubriken, mit denen Sie die Funktionsfähigkeit des Programms überwachen können (siehe Status).
  - Das Fenster **Status** bietet die Möglichkeit auf einen Blick zu sehen, welche Module aktiv sind und gibt Informationen über das letzte durchgeführte Update.
- *PC SICHERHEIT*: Hier finden Sie die Komponenten, mit denen Sie Dateien auf Ihrem Computersystem auf Viren und Malware prüfen.
  - Die Rubrik System-Scanner bietet Ihnen die Möglichkeit, die Direktsuche auf einfache Art und Weise zu konfigurieren bzw. zu starten (siehe System-Scanner). Vordefinierte Profile ermöglichen einen Suchlauf mit bereits angepassten Standardoptionen. Genau so ist es möglich mit Hilfe der Manuellen Auswahl (wird gespeichert) bzw. durch die Erstellung benutzerdefinierter Profile, die Suche nach Viren und unerwünschten Programmen auf Ihre persönlichen Bedürfnisse anzupassen.
  - Die Rubrik Echtzeit-Scanner zeigt Ihnen Informationen zu überprüften Dateien, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".
- *INTERNET SICHERHEIT*: Hier finden Sie die Komponenten, mit denen Sie Ihr Computersystem vor Viren und Malware aus dem Internet sowie vor unerwünschten Netzzugriffen schützen.
  - Die Rubrik FireWall bietet Ihnen die Möglichkeit, die Grundeinstellungen der FireWall zu konfigurieren. Es werden Ihnen außerdem die aktuelle Datenübertragungsrate und alle aktiven Anwendungen angezeigt, die eine Netzwerkverbindung verwenden (siehe FireWall).
  - Die Rubrik Browser-Schutz zeigt Ihnen Informationen zu überprüften URLs und gefundenen Viren, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere

Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".
  - Die Rubrik Email-Schutz zeigt Ihnen die vom Email-Schutz überprüften Emails, deren Eigenschaften sowie weitere statistische Daten.

- *KINDER SCHUTZ*: Hier finden Sie Werkzeuge, mit denen Sie ein sicheres Web-Erlebnis für Ihre Kinder ermöglichen.
  - Soziale Netzwerke: Die Rubrik Soziale Netzwerke leitet Sie zur Avira Kinderschutz für soziale Netzwerke Anwendung weiter. Avira Kinderschutz für soziale Netzwerke informiert Eltern über die Online-Aktivitäten ihrer Kinder. Das System prüft die Konten der sozialen Netzwerke auf Kommentare, Fotos usw., die dem Ruf ihres Kindes schaden könnten oder die darauf hinweisen könnten, dass Ihr Kind gefährdet ist.
- *MOBILER SCHUTZ*: Über die Kategorie Avira Free Android Security können Sie online auf Ihre Android-Geräte zugreifen.
  - Mit Avira Free Android Security verwalten Sie all Ihre Geräte, die mit dem Android-Betriebssystem arbeiten.
- *VERWALTUNG*: Hier finden Sie Werkzeuge, mit denen Sie verdächtige oder von Viren betroffene Dateien isolieren und administrieren sowie wiederkehrende Aufgaben planen können.
  - Hinter der Rubrik Quarantäne verbirgt sich der so genannte Quarantänemanager. Die zentrale Stelle für bereits in Quarantäne gestellte Dateien oder aber für verdächtige Dateien, die Sie in Quarantäne stellen möchten (siehe Quarantäne). Zudem besteht die Möglichkeit, eine ausgewählte Datei per Email an das Avira Malware Research Center zu senden.
  - Die Rubrik Planer bietet Ihnen die Möglichkeit, zeitlich gesteuerte Prüf- und Update-Aufträge zu erstellen und bestehende Aufträge anzupassen bzw. zu löschen (siehe Planer).
  - Die Rubrik Berichte bietet Ihnen die Möglichkeit, sich die Ergebnisse der durchgeführten Aktionen anzusehen (siehe Berichte).
  - Die Rubrik Ereignisse bietet Ihnen die Möglichkeit, sich über die Ereignisse zu informieren, die von den Modulen des Programms erzeugt werden (siehe Ereignisse).

Schaltflächen und Links

Folgende Schaltflächen und Links sind verfügbar.

Schaltfläche/Link	Tastaturbefehl	Beschreibung
Konfiguration	**F8**	Der Konfigurations-Dialog der Rubrik wird aufgerufen.
	F1	Das entsprechende Online-Hilfethema wird geöffnet.
Zum Avira Experts Market		Die Webseite Experts Market öffnet sich. Dort können Sie um Hilfe bitten oder anderen Anwendern Ihre Hilfe anbieten.

7.2 Datei

7.2.1 Beenden

Der Menüpunkt **Beenden** im Menü **Datei** schließt das Control Center.

7.3 Ansicht

7.3.1 Status

Der Startbildschirm des Control Centers **Status** bietet die Möglichkeit auf einen Blick zu sehen, ob Ihr Computersystem geschützt ist und welche Avira Module aktiv sind. Desweiteren gibt das Fenster **Status** Informationen über das letzte durchgeführte Update. Zudem ist ersichtlich, ob Sie Inhaber einer gültigen Lizenz sind.

- PC Sicherheit: Echtzeit-Scanner, Letzter Suchlauf, Letztes Update, Ihr Produkt ist aktiviert
- Internet Sicherheit: Browser-Schutz, Email-Schutz, FireWall, Spielmodus, Präsentationsmodus, Experts Market

> **Hinweis**
> Die Benutzerkontensteuerung (UAC) benötigt Ihre Zustimmung zur Aktivierung oder Deaktivierung der Echtzeit-Scanner, FireWall, Browser-Schutz und Email-Schutz Dienste in Betriebssystemen ab Windows Vista.

PC Sicherheit

In diesem Bereich erhalten Sie Informationen zum aktuellen Status der Dienste und Schutzfunktionen, die Ihren Computer lokal vor Viren und Malware schützen.

Echtzeit-Scanner

In diesem Bereich werden Sie zum aktuellen Status des Echtzeit-Scanner informiert.

Sie können den Echtzeit-Scanner mithilfe der Schaltfläche **An/Aus** aktivieren und deaktivieren. Für weitere Optionen zum Echtzeit-Scanner klicken Sie in der Navigationsleiste **Echtzeit-Scanner**. Zunächst erhalten sie Statusinformationen über zuletzt gefundene Malware und infizierte Dateien. Klicken Sie **Konfiguration**, um weitere Einstellungen vorzunehmen.

- **Konfiguration**: Sie gelangen in die Konfiguration, wo Sie Einstellungen für die Komponenten des Moduls Echtzeit-Scanners vornehmen können.

Folgende Möglichkeiten sind gegeben:

<table>
<tr><th>Symbol</th><th>Status</th><th>Option</th><th>Beschreibung</th></tr>
<tr><td>✅</td><td>Aktiviert</td><td>Deaktivieren</td><td>Der Echtzeit-Scanner Dienst ist aktiv, d.h. Ihr System wird ständig auf Viren und unerwünschte Programme überwacht.

Hinweis
Sie können den Echtzeit-Scanner Dienst deaktivieren. Beachten Sie jedoch, dass Sie bei deaktiviertem Echtzeit-Scanner nicht mehr vor Viren und unerwünschten Programmen geschützt sind. Alle Dateien können das System unbehelligt passieren und möglicherweise einen Schaden verursachen.</td></tr>
<tr><td>❗</td><td>Deaktiviert</td><td>Aktivieren</td><td>Der Echtzeit-Scanner Dienst ist deaktiviert, d.h. dass der Dienst geladen, jedoch nicht aktiv ist.

Warnung
Es wird nicht nach Viren und unerwünschten Programmen gesucht. Alle Dateien können das System unbehelligt passieren. Sie sind nicht vor Viren und unerwünschten Programmen geschützt.

Hinweis
Um wieder vor Viren und unerwünschten Programmen geschützt zu sein klicken Sie bitte die AN/AUS Schaltfläche, neben dem Echtzeit-Scanner im Bereich PC Sicherheit.</td></tr>
</table>



	Dienst gestoppt	**Starten**	Der Echtzeit-Scanner Dienst ist gestoppt. **Warnung** Es wird nicht nach Viren und unerwünschten Programmen gesucht. Alle Dateien können das System unbehelligt passieren. Sie sind nicht vor Viren und unerwünschten Programmen geschützt. **Hinweis** Um wieder vor Viren und unerwünschten Programmen geschützt zu sein klicken Sie bitte die **AN/AUS** Schaltfläche, neben dem **Echtzeit-Scanner** im Bereich *PC Sicherheit*. Der aktuelle Status sollte nun **Aktiviert** anzeigen.
	Unbekannt	**Hilfe**	Dieser Status wird angezeigt, wenn ein unbekannter Fehler auftritt. Wenden Sie sich bitte in diesem Fall an unseren Support.

Letzter Suchlauf

In diesem Bereich erhalten Sie Informationen zur zuletzt durchgeführten Systemprüfung. Bei einer vollständigen Systemprüfung werden alle Festplatten Ihres Computers umfassend geprüft. Dabei werden alle Such- und Prüfverfahren mit Ausnahme der Integritätsprüfung von Systemdateien eingesetzt: Standardsuche über Dateien, Prüfung von Registry und Bootsektoren, Suche nach Rootkits und aktiver Malware etc.

Folgende Details werden angezeigt:

- das Datum der letzten vollständigen Systemprüfung

Folgende Möglichkeiten sind gegeben:

Systemprüfung	Option	Beschreibung
Nicht ausgeführt	**System prüfen**	Seit der Installation wurde noch keine vollständige Systemprüfung durchgeführt. **Warnung** Der Status des Systems ist ungeprüft. Es besteht die Möglichkeit, dass sich Viren oder unerwünschte Programme auf Ihrem Computer befinden. **Hinweis** Um Ihren Computer zu prüfen, klicken Sie auf die Schaltfläche **System prüfen**.
Datum der letzten Systemprüfung, z.B. *18.09.2011*	**System prüfen**	Sie haben eine vollständige Systemprüfung zum angegebenen Datum durchgeführt. **Hinweis** Es wird empfohlen, den standardmäßig eingerichteten Prüfauftrag *Vollständige Systemprüfung* zu nutzen. Aktivieren Sie den Prüfauftrag **Vollständige Systemprüfung** im Planer.
Unbekannt	**Hilfe**	Dieser Status wird angezeigt, wenn ein unbekannter Fehler auftritt. Wenden Sie sich bitte in diesem Fall an unseren Support.

Letztes Update

In diesem Bereich erhalten Sie Informationen zum aktuellen Status Ihres zuletzt durchgeführten Updates.

Folgende Details werden angezeigt:

- das Datum des letzten Updates

  ▶ Klicken Sie die Schaltfläche **Konfiguration**, um weitere Einstellungen für das automatische Update vorzunehmen.

Folgende Möglichkeiten sind gegeben:

Symbol	Status	Option	Beschreibung
✅	*Datum der letzten Aktualisierung, z. B. 18.07.2011*	**Update starten**	Das Programm wurde innerhalb der letzten 24 Stunden aktualisiert. **Hinweis** Über die Schaltfläche **Update** starten bringen Sie Ihr Avira Produkt auf den aktuellsten Stand.
!	*Datum der letzten Aktualisierung, z. B. 18.07.2011*	**Update starten**	Seit der Aktualisierung sind bereits 24 Stunden vergangen, jedoch befinden Sie sich noch in dem von Ihnen gewählten Update-Erinnerungs-Zyklus. Dieser ist abhängig von den Einstellungen in der Konfiguration. **Hinweis** Über die Schaltfläche **Update starten** bringen Sie Ihr Avira Produkt auf den aktuellsten Stand.

	Nicht ausgeführt	**Update starten**	Seit der Installation wurde noch kein Update durchgeführt -oder- Seit der Installation wurde noch kein Update durchgeführt oder der von Ihnen gewählte Update-Erinnerungs-Zyklus wurde überschritten (siehe Konfiguration) und es wurde keine Aktualisierung durchgeführt oder die Virendefinitionsdatei ist älter als der von Ihnen gewählte Update-Erinnerungszyklus (siehe Konfiguration). **Hinweis** Über die Schaltfläche **Update starten** bringen Sie Ihr Avira Produkt auf den aktuellsten Stand.
		Nicht möglich	Bei abgelaufener Lizenz sind keine Updates möglich.

Ihr Produkt ist aktiviert

In diesem Bereich erhalten Sie Informationen zum aktuellen Status Ihrer Lizenz.

Folgende Möglichkeiten sind gegeben:

Vollversion

Symbol	Status	Option	Bedeutung
	Gültigkeitsdatum der aktuellen Lizenz für eine Vollversion, z.B. 31.10.2011	**Erneuern**	Sie sind in Besitz einer gültigen Lizenz für Ihr Avira Produkt. Über die Schaltfläche **Erneuern** gelangen Sie in den Avira Online-Shop. Dort haben Sie die Möglichkeit, Ihre aktuelle Lizenz Ihren Bedürfnissen anzupassen und ein Upgrade auf Avira Premium durchzuführen.
	Gültigkeitsdatum der aktuellen Lizenz für eine Vollversion, z.B. 31.10.2011	**Erneuern**	Sie sind in Besitz einer gültigen Lizenz für Ihr Avira Produkt. Der Lizenzierungszeitraum beläuft sich jedoch nur noch auf 30 oder weniger Tage. Über die Schaltfläche **Erneuern** gelangen Sie in den Avira Online-Shop. Dort haben Sie die Möglichkeit, Ihre aktuelle Lizenz zu verlängern.
	Lizenz abgelaufen am: z. B. 31.08.2011	**Kaufen**	Ihre Lizenz für Ihr Avira Produkt ist abgelaufen. Über die Schaltfläche **Kaufen** gelangen Sie in den Avira Online-Shop. Dort haben Sie die Möglichkeit, eine aktuelle Lizenz zu erwerben. **Warnung** Ist Ihre Lizenz abgelaufen, sind keine mehr Updates möglich. Die Schutzfunktionen des Programms sind deaktiviert und können nicht mehr aktiviert werden.

Evaluationslizenz

Symbol	Status	Option	Bedeutung
✅	*Gültigkeitsdatum der Evaluationslizenz, z. B. 31.10.2011*	**Kaufen**	Sie verfügen über eine Evaluationslizenz und haben so die Möglichkeit, Ihr Avira Produkt für einen bestimmten Zeitraum in seinem vollen Funktionsumfang zu testen. Über die Schaltfläche **Kaufen** gelangen Sie in den Avira Online-Shop. Dort haben Sie die Möglichkeit, eine aktuelle Lizenz zu erwerben.
!	*Gültigkeitsdatum der Evaluationslizenz, z. B. 31.10.2011*	**Erneuern**	Sie verfügen über eine Evaluationslizenz. Der Lizenzierungszeitraum beläuft sich jedoch nur noch auf 30 oder weniger Tage. Über die Schaltfläche **Erneuern** gelangen Sie in den Avira Online-Shop. Dort haben Sie die Möglichkeit, eine aktuelle Lizenz zu erwerben.
✕	*Evaluationslizenz abgelaufen am: 31.10.2011*	**Kaufen**	Ihre Lizenz für Ihr Avira Produkt ist abgelaufen. Über die Schaltfläche **Kaufen** gelangen Sie in den Avira Online-Shop. Dort haben Sie die Möglichkeit, eine aktuelle Lizenz zu erwerben. Warnung Ist Ihre Lizenz abgelaufen, sind keine mehr Updates möglich. Die Schutzfunktionen des Programms sind deaktiviert und können nicht mehr aktiviert werden.

Internet Sicherheit

In diesem Bereich erhalten Sie Informationen zum aktuellen Status der Dienste, die Ihren Computer vor Viren und Malware aus dem Internet schützen.

- **FireWall**: Der Dienst kontrolliert die Kommunikationswege von und zu Ihrem Computer.
- **Browser-Schutz**: Der Dienst prüft die Daten, die beim 'Surfen' im Internet übertragen und in Ihren Webbrowser geladen werden (Überwachung der Ports 80, 8080, 3128).
- **Email-Schutz**: Der Dienst prüft Emails und deren Anhänge auf Viren und Malware.
- **Spielmodus**: Bei aktivierter Option schaltet Ihr Avira Produkt automatisch in den Spielmodus um, wenn auf Ihrem Computer eine Anwendung im Vollbildmodus ausgeführt wird.

- **Experts Market**: Durch Klicken der Schaltfläche **Zum Avira Experts Market**, werden Sie zur Online-Plattform *Experts Market* weitergeleitet. Dort können Sie Experten finden, die Ihnen bei Computer-Problemen helfen, oder Sie selbst bieten Ihre Dienste als Experte an.

Weitere Optionen zu den Diensten sind in einem Kontextmenü sichtbar, wenn Sie das Symbol der Konfiguration neben der Schaltfläche **AN/AUS** klicken.

- **Konfiguration**: Sie gelangen in die Konfiguration, wo Sie Einstellungen für die Komponenten des Dienstes vornehmen können.

Folgende Möglichkeiten sind gegeben: *Dienste*

Symbol	Status	Status Dienst	Option	Bedeutung
✅	*OK*	*Aktiviert*	**Deaktivieren**	Alle Dienste zur Internet Sicherheit sind aktiv. **Hinweis** Sie können einen Dienst deaktivieren, indem Sie die Schaltfläche **AN/AUS** klicken. Beachten Sie jedoch, dass Sie bei einem deaktivierten Dienst nicht mehr vollständig vor Viren und Malware geschützt sind.
❗	*Eingeschränkt*	*Deaktiviert*	**Aktivieren**	Ein Dienst ist deaktiviert, d.h. der Dienst ist gestartet, jedoch nicht aktiv. **Warnung** Ihr Computersystem wird nicht vollständig überwacht. Es besteht die Möglichkeit, dass Viren und unerwünschte Programme in Ihr Computersystem gelangen. **Hinweis** Um den Dienst zu aktivieren, klicken Sie die Schaltfläche **AN/AUS** neben dem entsprechenden Dienst.

✖	*Warnung*	*Dienst gestoppt*	**Starten**	Ein Dienst wurde gestoppt **Warnung** Ihr Computersystem wird nicht vollständig überwacht. Es besteht die Möglichkeit, dass Viren und unerwünschte Programme in Ihr Computersystem gelangen. **Hinweis** Um den Dienst zu starten und Ihr Computersystem überwachen zu lassen, klicken Sie die Schaltfläche **AN/AUS**. Der Dienst wird gestartet und aktiviert.
		Unbekannt	**Hilfe**	Dieser Status wird angezeigt, wenn ein unbekannter Fehler auftritt. Wenden Sie sich bitte in diesem Fall an unseren Support.

7.3.2 Spielmodus

Wenn Sie auf Ihrem Computer Anwendungen ausführen, die den Vollbildmodus benötigen, können Sie durch Aktivierung des Spielmodus Desktop-Mitteilungen und Hinweise wie Popup-Fenster und Produkt-Benachrichtigungen gezielt unterdrücken.

Sie haben die Möglichkeit, den Spielmodus mit einem Klick auf die Schaltfläche **AN/AUS** zu aktivieren bzw. im automatischen Modus zu halten. Voreingestellt ist der Spielmodus mit **Automatik** und wird in grüner Farbe dargestellt. Mit dieser Voreinstellung schaltet Ihr Avira Produkt automatisch auf den Spielmodus um, wenn Sie eine Anwendung im Vollbildmodus ausführen.

- Klicken Sie die Schaltfläche links neben **AUS**, um den Spielmodus zu aktivieren.

↳ Der Spielmodus ist eingeschaltet, und die Schaltfläche wird in gelber Farbe dargestellt.

> **Hinweis**
> Wir empfehlen, den voreingestellten Status **AUS** mit seiner automatischen Erkennung von Anwendungen im Vollbildmodus nur temporär zu ändern, da Sie im Spielmodus keine sichtbaren Desktop-Mitteilungen und Warnungen über Netzwerkzugriffe und eventuelle Gefahren erhalten.

7.3.3 System-Scanner

Die Rubrik **System-Scanner** bietet Ihnen die Möglichkeit, die Direktsuche, d.h. die Suche auf Verlangen, auf einfache Art und Weise zu konfigurieren bzw. zu starten. Vordefinierte Profile ermöglichen einen Suchlauf mit bereits angepassten Standardoptionen. Ebenso ist es möglich mit Hilfe der Manuellen Auswahl bzw. durch die Erstellung benutzerdefinierter Profile, die Suche nach Viren und unerwünschten Programmen auf Ihre persönlichen Bedürfnisse anzupassen. Die gewünschte Aktion ist entweder per Auswahl über das Symbol in der Symbolleiste, per Tastaturbefehl oder aber über das Kontextmenü erreichbar. Einen Suchlauf starten Sie über den Punkt Suchlauf mit dem ausgewählten Profil starten.

Die Darstellung und Handhabung der editierbaren Profile entspricht der des Windows-Explorers. Jeder Ordner im Hauptverzeichnis entspricht einem Profil. Zu durchsuchende Ordner bzw. Dateien sind mit einem Haken vor dem zu durchsuchenden Ordner bzw. der zu durchsuchenden Datei markiert bzw. können markiert werden.

- Um Verzeichnisse zu wechseln, doppelklicken Sie auf das gewünschte Verzeichnis.
- Um Laufwerke zu wechseln, doppelklicken Sie auf den gewünschten Laufwerksbuchstaben.
- Zum Auswählen von Ordnern und Laufwerken können Sie auf das Kästchen vor einem Ordner- bzw. Laufwerkssymbol klicken oder die Auswahl über das Kontextmenü vornehmen.
- Mit Hilfe der Bildlaufleiste und den Bildlaufpfeilen können Sie durch die Menüstruktur navigieren.

Vordefinierte Profile

Für einen Suchlauf stehen Ihnen bereits vordefinierte Profile zur Verfügung.

> **Hinweis**
> Diese Profile sind schreibgeschützt und können nicht verändert oder gelöscht werden. Um ein Profil auf Ihre Bedürfnisse anzupassen, wählen Sie für einen einmaligen Suchlauf den Ordner Manuelle Auswahl bzw. Neues Profil erstellen

für die Erstellung eines benutzerdefinierten Profils, welches gespeichert werden kann.

Hinweis
Die Suchoptionen für die vordefinierte Profile können unter Konfiguration > System-Scanner > Suche > Dateien eingestellt werden. Diese Einstellungen können Sie auf Ihre Bedürfnisse anpassen.

Lokale Laufwerke

Alle lokalen Laufwerke auf Ihrem System werden nach Viren bzw. unerwünschten Programmen durchsucht.

Lokale Festplatten

Alle lokalen Festplatten auf Ihrem System werden nach Viren bzw. unerwünschten Programmen durchsucht.

Wechsellaufwerke

Alle verfügbaren Wechsellaufwerke Ihres Systems werden nach Viren bzw. unerwünschten Programmen durchsucht.

Windows Systemverzeichnis

Das Windows Systemverzeichnis Ihres Systems wird nach Viren bzw. unerwünschten Programmen durchsucht.

Vollständige Systemprüfung

Alle lokalen Festplatten Ihres Computers werden nach Viren bzw. unerwünschten Programmen durchsucht. Bei der Suche werden alle Such- und Prüfverfahren mit Ausnahme der Integritätsprüfung von Systemdateien eingesetzt: Standardsuche über Dateien, Prüfung von Registry und Bootsektoren, Suche nach Rootkits und aktiver Malware etc. (siehe System Scanner > Überblick). Die Prüfverfahren werden unabhängig von den Einstellungen des System-Scanners in der Konfiguration unter System Scanner > Suche: Weitere Einstellungen ausgeführt.

Schnelle Systemprüfung

Die wichtigsten Ordner Ihres Systems (die Verzeichnisse *Windows*, *Programme*, *Dokumente und Einstellungen\Default User*, *Dokumente und Einstellungen\All Users*) werden nach Viren bzw. unerwünschten Programmen durchsucht.

Meine Dokumente

Der Standardspeicherort "Eigene Dateien" des eingeloggten Benutzers wird nach Viren bzw. unerwünschten Programmen durchsucht.

Hinweis
"*Eigene Dateien*" ist unter Windows ein Verzeichnis im Profil des Benutzers, das als Standardspeicherort für gespeicherte Dokumente verwendet wird. In der Standardeinstellung befindet sich das Verzeichnis unter *C:\Dokumente und Einstellungen\[Benutzername]\Eigene Dateien*.

Aktive Prozesse

Alle laufenden Prozesse werden nach Viren bzw. unerwünschten Programmen durchsucht.

Suche nach Rootkits und Aktiver Malware

Der Computer wird nach Rootkits und nach aktiven (laufenden) Schadprogrammen durchsucht. Dabei werden alle laufenden Prozesse geprüft.

Hinweis
Im interaktiven Modus haben Sie mehrere Auswahlmöglichkeiten, wie mit dem Fund weiter verfahren werden soll. Im automatischen Modus wird der Fund in der Reportdatei vermerkt.

Hinweis
Die Rootkits-Suche ist unter Windows XP 64 Bit nicht verfügbar!

Manuelle Auswahl

Wenn Sie die Suche auf Ihre Bedürfnisse abstimmen möchten, wählen Sie diesen Ordner. Markieren Sie die gewünschten zu durchsuchenden Verzeichnisse und Dateien.

Hinweis
Das Profil **Manuelle Auswahl** dient dazu, Daten durchsuchen zu können, ohne erst ein neues Profil zu erstellen.

Benutzerdefinierte Profile

Die Erstellung eines neuen Profils ist über die Symbolleiste, per Tastaturbefehl oder über das Kontextmenü möglich.

Neue Profile können unter dem von Ihnen gewünschten Namen gespeichert werden und sind zusätzlich zum manuell gesteuerten Suchlauf für die Erstellung von zeitgesteuerten Suchläufen mit Hilfe des Planer nützlich.

Symbolleiste und Tastaturbefehle

Symbol	Tastaturbefehl	Beschreibung
	F3	**Suchlauf mit dem ausgewählten Profil starten** Das markierte Profil wird nach Viren bzw. unerwünschten Programmen durchsucht.
	F6	**Suchlauf mit dem ausgewählten Profil als Administrator starten** Das markierte Profil wird mit administrativen Rechten durchsucht.
+	**Einf**	**Neues Profil erstellen** Ein neues Profil wird erstellt.
	F2	**Ausgewähltes Profil umbenennen** Gibt dem markierten Profil den von Ihnen gewählten Namen.
	F4	**Desktopverknüpfung für das ausgewählte Profil erstellen** Erstellt eine Verknüpfung des markierten Profils auf dem Desktop.
×	**Entf**	**Ausgewählte(s) Profil(e) löschen** Das ausgewählte Profil wird unwiderruflich gelöscht.

Kontextmenü

Das Kontextmenü für diese Rubrik erhalten Sie, indem Sie sich mit der Maus ein gewünschtes Profil markieren und die rechte Maustaste gedrückt halten.

Suchlauf starten

Das markierte Profil wird nach Viren bzw. unerwünschten Programmen durchsucht.

Suchlauf starten (Administrator)

(Diese Funktion ist nur unter Windows Vista verfügbar. Zur Ausführung dieser Aktion werden Administratorrechte benötigt.)

Das markierte Profil wird nach Viren bzw. unerwünschten Programmen durchsucht.

Neues Profil erstellen

Ein neues Profil wird erstellt. Markieren Sie die Verzeichnisse und Dateien, die geprüft werden sollen.

Profil umbenennen

Gibt dem markierten Profil den von Ihnen gewählten Namen.

> **Hinweis**
> Dieser Eintrag ist im Kontextmenü nicht auswählbar, wenn ein vordefiniertes Profil ausgewählt ist.

Profil löschen

Das ausgewählte Profil wird unwiderruflich gelöscht.

> **Hinweis**
> Dieser Eintrag ist im Kontextmenü nicht auswählbar, wenn ein vordefiniertes Profil ausgewählt ist.

Dateifilter

Standard:

Bedeutet, dass die Dateien entsprechend der Einstellung in der Gruppe Dateien der Konfiguration geprüft werden. Diese Einstellung können Sie in der Konfiguration auf Ihre Bedürfnisse anpassen. Zur Konfiguration gelangen Sie über die Schaltfläche bzw. den Link Konfiguration.

Prüfe alle Dateien:

Alle Dateien werden geprüft, unabhängig von der Einstellung in der Konfiguration.

Benutzerdefiniert:

Es wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Suchlauf durchsucht werden. Bei den Endungen sind Standardeinträge vorgegeben. Es lassen sich aber auch Einträge hinzufügen oder entfernen.

> **Hinweis**
> Dieser Eintrag ist im Kontextmenü nur auswählbar, wenn Sie sich mit der Maus

über einem Kontrollkästchen befinden.
Die Auswahl der Option ist bei vordefinierten Profilen nicht möglich.

Markiere

Mit Unterverzeichnissen:

Im markierten Knoten wird alles geprüft (schwarzes Häkchen).

Ohne Unterverzeichnisse:

Im markierten Knoten werden nur die Dateien geprüft (grünes Häkchen).

Nur Unterverzeichnisse:

Im markierten Knoten werden nur die Unterverzeichnisse geprüft, nicht die Dateien, die sich in dem Knoten befinden (graues Häkchen, Unterverzeichnisse haben schwarzes Häkchen).

Keine Auswahl:

Auswahl wird aufgehoben, der aktuell markierte Knoten wird nicht geprüft (kein Häkchen).

Hinweis
Dieser Eintrag ist im Kontextmenü nur auswählbar, wenn Sie sich mit der Maus über einem Kontrollkästchen befinden.
Die Auswahl der Option ist bei vordefinierten Profilen nicht möglich.

Desktopverknüpfung erstellen

Erstellt eine Verknüpfung des markierten Profils auf dem Desktop.

Hinweis
Dieser Eintrag ist im Kontextmenü nicht auswählbar, wenn das Profil Manuelle Auswahl ausgewählt ist, da die Einstellungen der Manuellen Auswahl nicht auf Dauer gespeichert werden.

7.3.4 Echtzeit-Scanner

Die Rubrik **Echtzeit-Scanner** zeigt Ihnen Informationen zu überprüften Dateien sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".

Hinweis
Ist der Echtzeit Scanner Dienst nicht gestartet, ist die Schaltfläche neben dem

Modul in gelber Farbe dargestellt. Sie haben trotzdem die Möglichkeit, sich die Reportdatei des Echtzeit-Scanners anzeigen zu lassen.

Symbolleiste

Symbol	**Beschreibung**
	Reportdatei anzeigen Die Reportdatei des Echtzeit-Scanners wird angezeigt.
	Statistikdaten zurücksetzen Die statistischen Informationen dieser Rubrik werden auf Null gesetzt.

Angezeigte Informationen

Letzte infizierte Datei

Zeigt den Namen und Ort der zuletzt vom Echtzeit Scanner gefundene Datei.

Letzte gefundene Malware

Nennt den Namen des zuletzt gefundenen Virus bzw. unerwünschten Programms.

Symbol	**Beschreibung**
Informationen zu Viren	Beim Klick auf das Symbol bzw. den Link werden Ihnen, bei einer bestehenden Internetverbindung, detaillierte Informationen zum Virus bzw. unerwünschten Programm angezeigt.

Letzte überprüfte Datei

Zeigt den Namen und Pfad der zuletzt vom Echtzeit Scanner überprüften Datei.

Statistik

Anzahl Dateien

Zeigt die Anzahl der bisher durchsuchten Dateien.

Anzahl gefundener Malware

Zeigt die Anzahl der bisher gefundenen Viren und unerwünschten Programme.

Anzahl verdächtiger Dateien

Zeigt die Anzahl der Dateien, die von der Heuristik gemeldet wurden.

Anzahl gelöschter Dateien

Zeigt die Anzahl der bisher gelöschten Dateien.

Anzahl reparierter Dateien

Zeigt die Anzahl der bisher reparierten Dateien.

Anzahl verschobener Dateien

Zeigt die Anzahl der bisher verschobenen Dateien.

Anzahl umbenannter Dateien

Zeigt die Anzahl der bisher umbenannten Dateien.

7.3.5 FireWall

Windows-Firewall (ab Windows 7)

Avira verwaltet die Windows-Firewall mithilfe des Control- und Konfigurationcenters.

Die Rubrik FireWall bietet Ihnen die Möglichkeit, den Status der Windows-Firewall zu überprüfen und die empfohlenen Einstellungen wiederherzustellen, indem Sie die Schaltfläche **Problem beheben** klicken.

7.3.6 Browser-Schutz

Die Rubrik **Browser-Schutz** zeigt Ihnen Informationen zu überprüften URLs, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".

Symbolleiste

Symbol	Beschreibung
	Reportdatei anzeigen Die Reportdatei des Browser-Schutzes wird angezeigt.
	Statistikdaten zurücksetzen Die statistischen Informationen dieser Rubrik werden auf Null gesetzt.

Angezeigte Informationen

Letzte betroffene URL

Zeigt die zuletzt vom Browser-Schutz gefundene URL.

Letzter gefundener Virus oder unerwünschtes Programm

Nennt den Namen des zuletzt gefundenen Virus bzw. unerwünschten Programms.

Symbol/Link	Beschreibung
Informationen zu Viren	Beim Klick auf das Symbol bzw. den Link werden Ihnen, bei einer bestehenden Internetverbindung, detaillierte Informationen zum Virus bzw. unerwünschten Programm angezeigt.

Letzte überprüfte URL

Zeigt den Namen und Pfad der zuletzt vom Browser-Schutz überprüften URL.

Statistik

Anzahl geprüfter URLs

Zeigt die Anzahl der bisher geprüften URLs.

Anzahl Meldungen

Zeigt die Anzahl der bisher gefundenen Viren und unerwünschten Programme.

Anzahl blockierter URLs

Zeigt die Anzahl der bisher blockierten URLs.

Anzahl ignorierter URLs

Zeigt die Anzahl der bisher ignorierten URLs.

7.3.7 Email-Schutz

Die Rubrik **Email-Schutz** zeigt Ihnen die vom Email-Schutz überprüften Emails, deren Eigenschaften sowie weitere statistische Daten.

> **Hinweis**
> Ist der Email Schutz Dienst nicht gestartet, ist die Schaltfläche neben dem Modul in gelber Farbe dargestellt. Es besteht jedoch noch die Möglichkeit, sich die Reportdatei des Email-Schutzes anzeigen zu lassen. Steht in Ihrem Avira Produkt dieser Dienst nicht zur Verfügung, ist die Schaltfläche ausgegraut.

> **Hinweis**
> Der Ausschluss einzelner Email-Adressen von der Prüfung auf Malware bezieht sich natürlich nur auf eingehende Emails. Um die Prüfung ausgehender Emails abzuschalten, deaktivieren Sie die Prüfung ausgehender Emails in der Konfiguration unter Email Schutz > Suche.

Symbolleiste

Symbol	Beschreibung
	Reportdatei anzeigen Die Reportdatei des Email-Schutzes wird angezeigt.
	Eigenschaften der ausgewählten Email anzeigen Öffnet ein Dialogfenster mit näheren Informationen zur ausgewählten Email.
	Email-Adresse nicht mehr auf Malware prüfen Die ausgewählte Email-Adresse wird in Zukunft nicht mehr auf Viren und unerwünschte Programme überprüft. Sie können diese Einstellung in der Konfiguration unter **Email-Schutz > Allgemeines > Ausnahmen** wieder rückgängig machen (siehe Ausnahmen).
	Ausgewählte Email(s) löschen Die ausgewählte Email wird aus dem Zwischenspeicher gelöscht. Die Datei bleibt jedoch in Ihrem Email-Programm erhalten.

	**Statistikdaten zurücksetzen** Die statistischen Informationen dieser Rubrik werden auf Null gesetzt.

Geprüfte Emails

In diesem Bereich werden die Emails angezeigt, die vom Email-Schutz überprüft wurden.

Symbol	Beschreibung
	Es wurde kein Virus oder unerwünschtes Programm gefunden.
	Es wurde ein Virus oder unerwünschtes Programm gefunden.

Typ

Zeigt das Protokoll an, das genutzt wurde, um die Email zu empfangen oder zu senden:

- POP3: über POP3 empfangene Email
- IMAP: über IMAP empfangene Email
- SMTP: über SMTP gesendete Email

Absender/Empfänger

Zeigt die Absenderadresse der Email.

Betreff

Zeigt den Betreff der empfangenen Email.

Datum/Uhrzeit

Zeigt wann die Email überprüft wurde.

> **Hinweis**
> Weitere Informationen zu einer Email erhalten Sie durch einen Doppelklick auf die gewünschte Email.

Statistik

Email-Aktion

Zeigt die Aktion, die durchgeführt wird, wenn der Email-Schutz einen Virus oder ein unerwünschtes Programm in einer Email findet. Im interaktiven Modus ist hier keine

Anzeige verfügbar, da Sie selbst wählen können, welches Vorgehen bei einem Fund durchgeführt wird.

> **Hinweis**
> Diese Einstellung können Sie in der Konfiguration auf Ihre Bedürfnisse anpassen. Zur Konfiguration gelangen Sie über die Schaltfläche bzw. den Link Konfiguration.

Betroffene Anlagen

Zeigt die Aktion, die durchgeführt wird, wenn der Email-Schutz einen Virus oder ein unerwünschtes Programm in einem betroffenen Anhang findet. Im interaktiven Modus ist hier keine Anzeige verfügbar, da Sie selbst wählen können, welches Vorgehen bei einem Fund durchgeführt wird.

> **Hinweis**
> Diese Einstellung können Sie in der Konfiguration auf Ihre Bedürfnisse anpassen. Zur Konfiguration gelangen Sie über die Schaltfläche bzw. den Link Konfiguration.

Anzahl Emails

Zeigt die Anzahl der vom Email-Schutz durchsuchten Emails.

Letzte Meldung

Nennt den Namen des zuletzt gefundenen Virus bzw. unerwünschten Programms.

Anzahl Meldungen

Zeigt die Anzahl der bisher gefundenen und gemeldeten Viren und unerwünschten Programme.

Verdächtige Emails

Zeigt die Anzahl der Emails, die von der Heuristik gemeldet wurden.

Anzahl empfangener Emails

Zeigt die Anzahl der eingegangenen Emails.

Anzahl gesendeter Emails

Zeigt die Anzahl der ausgegangenen Emails.

Avira Kinderschutz für Soziale Netzwerke ist eine internetbasierte Anwendung, die die Online-Aktivitäten Ihrer Kinder beobachtet. Ihr einziger Zweck ist es, Ihr Bewusstsein und das Ihrer Kinder dafür zu schulen, welche Gefahren im Internet lauern und Ihre Kinder davor zu bewahren, Schaden zu nehmen.

Die Kinderschutz-Technologie überprüft die Konten Ihrer Kinder bei sozialen Netzwerken auf Kommentare, Fotos etc., die dem Ruf des Kindes schaden könnten oder die darauf hinweisen könnten, dass sich das Kind in Gefahr befindet.Es warnt Sie daraufhin vor fragwürdigen Freunden und möglicherweise gefährlichen Aktivitäten in dem sozialen Netzwerkkonto Ihres Kindes einschließlich

- Kontakte mit Fremden
- Cybermobbing
- unangemessene Inhalte
- Veröffentlichung privater Informationen
- unbedachte, möglicherweise den guten Ruf gefährdende Aktivitäten

Avira Kinderschutz für Soziale Netzwerke kann folgende soziale Netzwerke beobachten:

- Facebook
- MySpace
- Twitter
- Google+
- Formspring

Hinweis
Um die Online-Konten Ihrer Kinder beobachten zu können, brauchen Sie entweder ihre Zustimmung oder den Benutzernamen und das Passwort für das jeweilige Konto.

Weitere Informationen:
Ein Kinderschutz-Konto für Soziale Netzwerke erstellen
Mit einem bestehenden Kinderschutz-Konto für Soziale Netzwerke anmelden

7.3.8 Avira Android Security

Avira Android Security ist eine App zum Schutz vor Diebstahl und/oder Verlust. Die App bietet Funktionen, mit deren Hilfe Sie das mobile Gerät ausfindig machen können, wenn Sie es verlegt haben oder schlimmer noch: wenn es gestohlen wurde. Darüberhinaus erlaubt Ihnen die Anwendung, eingehende Anrufe oder SMS zu blockieren. Avira Android Security schützt Mobiltelefone und Smartphones, die mit dem Betriebssystem Android arbeiten.

Avira Android Security besteht aus zwei Komponenten:

- Die eigentliche App, die auf dem Android-Gerät installiert wird
- Die Avira Android-Webkonsole zur Registrierung und Steuerung der Funktionen

Avira Android Security ist eine kostenlose App, für die auch keine Lizenz erforderlich ist. Avira Android Security unterstützt alle wichtigen Marken, wie z.B. Samsung, HTC, LG und Motorola.

Weitere Informationen finden Sie auf unserer Webseite:

www.avira.de/android

7.3.9 Quarantäne

Der **Quarantänemanager** verwaltet betroffene Objekte (Dateien und Emails). Ihr Avira Produkt kann betroffene Objekte in einem speziellen Format in das Quarantäneverzeichnis verschieben. Sie können dann nicht mehr ausgeführt oder geöffnet werden.

> **Hinweis**
> Um Objekte in den Quarantänemanager zu verschieben, wählen Sie in der **Konfiguration** unter System-Scanner und Echtzeit-Scanner sowie Email-Schutz jeweils unter **Suche > Aktion bei Fund** die entsprechende Option für die Quarantäne, wenn Sie im **automatischen Modus** arbeiten.
> Alternativ können Sie im **interaktiven Modus** die entsprechende Option für die Quarantäne auswählen.

7.3.10 Symbolleiste, Tastaturbefehl und Kontextmenü

Symbol	Tastaturbefehl	Beschreibung
	F2	**Objekt(e) erneut prüfen** Ein markiertes Objekt wird erneut auf Viren und unerwünschte Programme überprüft. Dabei werden die Einstellungen der Direktsuche verwendet (siehe System Scanner).
	Enter	**Erweiterte Eigenschaften** Öffnet ein Dialogfenster mit näheren Detailinformationen zum gewählten Objekt. **Hinweis** Die Detailinformationen können auch mit Doppelklick auf ein Objekt geöffnet werden.

(Windows Vista)	**F3**	**Objekt(e) wiederherstellen** Ein markiertes Objekt wird wiederhergestellt. Danach befindet sich dieses Objekt wieder an seinem ursprünglichen Ort. **Hinweis** Diese Option ist für Objekte des Typs Email nicht verfügbar. **Warnung** Enorme Schäden im System durch Viren und unerwünschte Programme! Wenn Sie Dateien wiederherstellen: Stellen Sie sicher, dass nur solche Dateien wiederhergestellt werden, die durch einen erneuten Suchlauf gesäubert werden konnten. **Hinweis** Unter Windows Vista ist das Wiederherstellen von Objekten nur mit Administratorrechten möglich.
	F6	**Objekt(e) wiederherstellen nach...** Ein markiertes Objekt kann wieder an dem von Ihnen gewünschten Ort hergestellt werden. Wählen Sie diese Option, öffnet sich ein "Speichern unter" Dialog in dem der gewünschte Speicherort ausgewählt werden kann. **Warnung** Enorme Schäden im System durch Viren und unerwünschte Programme! Wenn Sie Dateien wiederherstellen: Stellen Sie sicher, dass nur solche Dateien wiederhergestellt werden, die durch einen erneuten Suchlauf gesäubert werden konnten.

+	**Einf**	**Datei zur Quarantäne hinzufügen** Halten Sie eine Datei für verdächtig, können Sie diese manuell über diese Option dem Quarantänemanager hinzufügen und bei Bedarf über die Option Objekt senden auf einen Webserver des Avira Malware Research Center zur Überprüfung hochladen.
	F4	**Objekt(e) senden** Das Objekt wird zur Überprüfung durch das Avira Malware Research Center auf einen Webserver von Avira Malware Research Center hochgeladen. Wenn Sie die Schaltfläche **Objekt senden** drücken, öffnet sich zunächst ein Dialog mit einem Formular zur Eingabe Ihrer Kontaktdaten. Geben Sie die Daten vollständig an. Wählen Sie einen Typ aus: **Verdächtige Datei** oder **Fehlalarm**. Drücken Sie **OK**, um die verdächtige Datei hochzuladen. **Hinweis** Die Größe der Dateien, die Sie hochladen, ist begrenzt auf 20 MB ungepackt oder 8 MB gepackt. **Hinweis** Sie können jeweils nur eine einzelne Datei hochladen.
×	**Entf**	**Objekt(e) löschen** Eine markierte Datei wird aus dem Quarantänemanager gelöscht. Die Datei kann nicht wiederhergestellt werden.
	F7	**Alle Eigenschaften exportieren** Die Eigenschaften des markierten Quarantäne-Objekts werden in eine Textdatei exportiert.

	F10	**Quarantäneverzeichnis öffnen** Öffnet den Ordner INFECTED.

Hinweis
Sie haben die Möglichkeit, Aktionen für mehrere markierte Objekte auszuführen.
Um mehrere Objekte zu markieren, halten Sie die Strg-Taste oder die Shift-Taste (Auswahl untereinander stehender Objekte) gedrückt, während Sie die Objekte im Quarantänemanager auswählen. Um alle angezeigten Objekte auszuwählen, drücken Sie Strg + A.
Bei der Aktion Eigenschaften anzeigen ist die Ausführung für mehrfache Objektauswahl nicht möglich. Die Mehrfachauswahl ist bei der Aktion Objekt senden nicht möglich, da jeweils nur eine Datei pro Upload hochgeladen werden kann.

7.3.11 Tabelle

Status

Ein in Quarantäne gestelltes Objekt kann unterschiedliche Status haben:

Symbol	Beschreibung
	Es wurde kein Virus oder unerwünschtes Programm gefunden, das Objekt ist "sauber".
	Es wurde ein Virus oder unerwünschtes Programm gefunden.
	Wurde eine verdächtige Datei dem Quarantänemanager über die Option Datei hinzufügen hinzugefügt, erhält sie dieses Hinweissymbol.

Typ

Bezeichnung	Beschreibung
Email	Beim gefundenen Objekt handelt es sich um eine Email.
Datei	Beim gefundenen Objekt handelt es sich um eine Datei.

Meldung

Zeigt den Namen der gefundenen Malware an.
Heuristische Funde sind mit dem Kürzel HEUR/ gekennzeichnet.

Quelle

Zeigt den Pfad an, unter dem das Objekt gefunden wurde.

Datum/Uhrzeit

Zeigt Datum und Uhrzeit des Funds an.

Detailinformationen

Dateiname

Vollständiger Pfad und Dateiname des Objekts

Quarantäne-Objekt

Dateiname des Quarantäne-Objekts

Wiederhergestellt

JA / NEIN

JA: Das Objekt wurde wiederhergestellt.

NEIN: Das Objekt wurde nicht wiederhergestellt.

Zu Avira hochgeladen

JA / NEIN

JA: Das Objekt wurde bereits zur Überprüfung durch das Avira Malware Research Center auf einen Webserver von Avira Malware Research Center hochgeladen.

NEIN: Das Objekt wurde noch nicht zur Überprüfung durch das Avira Malware Research Center auf einen Webserver von Avira Malware Research Center hochgeladen.

Betriebssystem

Windows XP/Vista Workstation: Die Malware wurde von einem Avira Desktop-Produkt ermittelt.

Suchengine

Versionsnummer der Suchengine

Virendefinitionsdatei

Versionsnummer der Virendefinitionsdatei

Meldung

Name der gefundenen Malware

Datum/Uhrzeit

Datum und Uhrzeit des Funds

7.3.12 Planer

Der **Planer** bietet Ihnen die Möglichkeit, zeitlich gesteuerte Prüf- und Update-Aufträge zu erstellen, sowie bestehende Aufträge anzupassen bzw. zu löschen.

In der Standardeinstellung nach der Installation ist folgender Auftrag angelegt:

- Prüfauftrag **Schnelle Systemprüfung** (Standardeinstellung): Wöchentlich wird automatisch eine schnelle Systemprüfung ausgeführt. Bei der schnellen Systemprüfung werden die wichtigsten Dateien und Ordner Ihres Computers nach Viren oder unerwünschten Programmen durchsucht. Den Prüfauftrag können Sie ändern; Es ist aber zu empfehlen, weitere Prüfaufträge anzulegen, die Ihren Bedürfnissen besser entsprechen.

Symbolleiste, Tastaturbefehl und Kontextmenü

Symbol	Tastaturbefehl	Kontextmenü
+	Einf	**Neuen Auftrag einfügen** Legt einen neuen Auftrag an. Ein Assistent führt Sie übersichtlich durch die notwendigen Einstellungen.
i	Enter	**Eigenschaften** Öffnet ein Dialogfenster mit näheren Informationen zum ausgewählten Auftrag.
	F2	**Auftrag ändern** Öffnet den Assistenten zum Erstellen und Ändern eines Auftrags.
×	Entf	**Auftrag löschen** Löscht die markierten Aufträge aus der Liste.

		Reportdatei anzeigen Die Reportdatei des Planer wird angezeigt.
	F3	Auftrag starten Startet einen markierten Auftrag aus der Liste.
	F4	Auftrag stoppen Stoppt einen gestarteten und markierten Auftrag.

Tabelle

Art des Auftrags

Symbol	Beschreibung
	Bei dem Auftrag handelt es sich um einen Update-Auftrag.
	Bei dem Auftrag handelt es sich um einen Prüfauftrag.

Name

Bezeichnung des Auftrags.

Aktion

Zeigt an, ob es sich bei dem Auftrag um einen **Suchlauf** handelt oder um ein **Update**.

Häufigkeit

Zeigt an, wie oft und wann der Auftrag gestartet wird.

Darstellungsmodus

Folgende Darstellungsmodi stehen zur Verfügung:

Unsichtbar: Der Auftrag wird im Hintergrund durchgeführt und ist nicht sichtbar. Dies gilt für Prüfaufträge sowie Update-Aufträge.

Minimiert: Das Auftragsfenster zeigt nur einen Fortschrittsbalken.

Maximiert: Das Auftragsfenster ist komplett sichtbar.

Aktiviert

Der Auftrag wird aktiviert, wenn Sie das Kontrollkästchen aktivieren.

Hinweis
Wenn als Auftragshäufigkeit Sofort eingestellt wurde, wird der Auftrag direkt nach der Aktivierung gestartet. Dies bietet Ihnen die Möglichkeit, den Auftrag nach Bedarf erneut zu starten.

Status

Zeigt den Status des Auftrags an:

Bereit: Der Auftrag ist bereit zur Ausführung.

Läuft: Der Auftrag wurde gestartet und befindet sich in Ausführung.

Aufträge mit dem Planer anlegen

Der Planungsassistent unterstützt Sie beim Planen, Konfigurieren und Anlegen

- einer zeitgesteuerten Suche nach Viren und unerwünschten Programmen
- eines zeitgesteuerten Updates über das Internet

Für beide Arten von Aufträgen müssen Sie angeben,

- den Namen und die Beschreibung des Auftrags
- wann der Auftrag gestartet werden soll
- wie oft der Auftrag ausgeführt werden soll
- den Darstellungsmodus des Auftrags

Häufigkeit des Auftrags

Option	Beschreibung
Sofort	Auftrag wird sofort nach Beenden des Planungsassistenten gestartet.
Täglich	Auftrag wird täglich zu einer bestimmten Uhrzeit gestartet, z.B. 22:00 Uhr.

Wöchentlich	Auftrag wird wöchentlich an einem bestimmten Tag oder an mehreren Wochentagen zu einer bestimmten Zeit gestartet, z.B. Dienstag und Freitag, 16:26 Uhr.
Intervall	Auftrag wird in einem bestimmten Intervall ausgeführt, z.B. alle 24 Stunden.
Einmalig	Auftrag wird nur einmal zu einem fest definierten Zeitpunkt ausgeführt, z.B. am 10.04.04 um 10:04 Uhr.
Login	Auftrag wird bei jedem Anmeldevorgang eines Benutzers von Windows ausgeführt.

Startzeitpunkt des Auftrags

Sie können einen Wochentag, ein Datum, eine Uhrzeit oder ein Intervall für den Startzeitpunkt des Auftrags festlegen. Dies wird nicht angezeigt, wenn Sie als Startzeitpunkt *Sofort* angegeben haben.

Je nach Auftragsart gibt es verschiedene Zusatzoptionen:

Auftrag zusätzlich bei Internet-Verbindung starten (DFÜ)

Zusätzlich zur festgelegten Häufigkeit wird der Auftrag bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.
Diese Option ist bei einem Update-Auftrag wählbar, der täglich, wöchentlich oder im Intervall durchgeführt werden soll.

Auftrag nachholen, wenn die Zeit bereits abgelaufen ist

Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
Diese Option ist sowohl bei einem Update-Auftrag, als auch bei einem Prüfauftrag wählbar, der täglich, wöchentlich, im Intervall oder einmalig durchgeführt werden soll.

Computer herunterfahren, wenn Auftrag ausgeführt wurde

Der Computer wird heruntergefahren, nachdem der Auftrag ausgeführt und beendet wurde. Die Option ist für Prüfaufträge im minimierten und maximierten Darstellungsmodus verfügbar.

> **Hinweis**
> Bei einem Prüfauftrag ist es im Dialogfenster Auswahl des Profils möglich, sowohl vordefinierte Standard-Profile als auch benutzerdefinierte Profile

auszuwählen. Das Profil Manuelle Auswahl wird immer mit der aktuellen Auswahl durchgeführt.

7.3.13 Berichte

In der Rubrik **Berichte** können Sie Ergebnisse der vom Programm durchgeführten Aktionen abrufen.

Symbolleiste, Tastaturbefehl und Kontextmenü

Symbol	Tastaturbefehl	Beschreibung
	Enter	**Bericht anzeigen** Öffnet ein Fenster, in dem das Ergebnis der markierten Aktion angezeigt wird. Beispielsweise das Ergebnis eines Suchlaufs.
	F3	**Reportdatei anzeigen** Zeigt die Reportdatei zum entsprechend markierten Bericht an.
	F4	**Reportdatei drucken** Öffnet den Windows Drucken Dialog zum Drucken der Reportdatei.
	Entf	**Bericht(e) löschen** Löscht den markierten Bericht sowie die dazugehörige Reportdatei.

Tabelle

Status

Symbol	Beschreibung
✅	Aktion Suchlauf: Kein Fund!
⚠	Aktion Suchlauf: Virenfund oder nicht erfolgreich beendet
⟳	Aktion Update: Update war erfolgreich
⟳	Aktion Update: Update ist fehlgeschlagen

Aktion

Zeigt die vorgenommene Aktion.

Ergebnis

Zeigt das Ergebnis der Aktion.

Datum/Uhrzeit

Zeigt das Datum sowie die Uhrzeit, wann der Bericht erstellt wurde.

Inhalt eines Berichts für einen Suchlauf

- *Datum des Suchlaufs:*

  Datum des Suchlaufs.
- *Startzeit des Suchlaufs:*

  Startzeit des Suchlaufs.
- *Benötigte Suchzeit::*

  Zeigt die Zeit im Format mm:ss an.
- *Prüfstatus:*

  Zeigt, ob der Prüfauftrag vollständig durchgeführt oder aber abgebrochen wurde.
- *Letzter Fund:*

  Name des zuletzt gefundenen Virus bzw. unerwünschten Programms.
- *Durchsuchte Verzeichnisse:*

  Anzahl der insgesamt durchsuchten Verzeichnisse.
- *Durchsuchte Dateien:*

  Anzahl der insgesamt durchsuchten Dateien.
- *Durchsuchte Archive:*

  Anzahl der durchsuchten Archive.

- *Versteckte Objekte:*

  Anzahl der insgesamt gefundenen versteckten Objekte.
- *Gefunden:*

  Anzahl der insgesamt entdeckten Viren und unerwünschten Programme.
- *Verdächtig:*

  Anzahl verdächtiger Dateien.
- *Warnungen:*

  Anzahl von Warnmeldungen zu Virenfunden.
- *Hinweise:*

  Anzahl der Hinweise die ausgegeben wurden, z.B. weitere Informationen, die während eines Suchlaufs auftreten können.
- *Repariert::*

  Anzahl der insgesamt reparierten Dateien.
- *Quarantäne:*

  Anzahl der insgesamt in Quarantäne verschobenen Dateien.
- *Umbenannt:*

  Anzahl der insgesamt umbenannten Dateien
- *Gelöscht:*

  Anzahl der insgesamt gelöschten Dateien.
- *Überschrieben:*

  Anzahl der insgesamt überschriebenen Dateien.

Hinweis
Rootkits haben die Eigenschaft, Prozesse und Objekte wie z.B. Registry-Einträge oder Dateien zu verstecken, jedoch ist nicht jedes verborgene Objekt ein zwingender Hinweis auf die Existenz eines Rootkits. Bei versteckten Objekten kann es sich auch um unschädliche Objekte handeln. Falls beim Suchlauf versteckte Objekte gefunden wurden und keine Warnmeldungen zu Virenfunden vorliegen, sollten Sie anhand des Reports ermitteln, um welche Objekte es sich handelt und weitere Informationen über die gefundenen Objekte einholen.

7.3.14 Ereignisse

Unter **Ereignisse** werden Ereignisse angezeigt, die von den verschiedenen Programmkomponenten erzeugt werden.

Die Ereignisse sind in einer Datenbank gespeichert. Sie haben die Möglichkeit, die Größe der Ereignisdatenbank zu begrenzen oder die Beschränkung der Datenbankgröße zu

deaktivieren (siehe Ereignisse). In der Standardeinstellung werden nur die Ereignisse der letzten 30 Tage gespeichert. Die Anzeige der Ereignisse wird automatisch aktualisiert, wenn Sie die Rubrik **Ereignisse** anwählen.

> **Hinweis**
> Eine automatische Aktualisierung der Anzeige bei Anwahl der Rubrik erfolgt nicht, wenn mehr als 20.000 Ereignisse in der Ereignisdatenbank gespeichert sind. Drücken Sie in diesem Fall **F5**, um die Ereignisanzeige zu aktualisieren.

Symbolleiste, Tastaturbefehl und Kontextmenü

Symbol	Tastaturbefehl	Beschreibung
	Enter	**Ausgewähltes Ereignis anzeigen** Öffnet ein Fenster, in dem das Ergebnis einer ausgewählten Aktion angezeigt wird. Zum Beispiel das Ergebnis eines Prüflaufes.
	F3	**Ausgewählte(s) Ereignis(se) exportieren** Exportiert ausgewählte Ereignisse.
	Entf	**Ausgewählte(s) Ereignis(se) löschen** Löscht ein ausgewähltes Ereignis.

> **Hinweis**
> Sie haben die Möglichkeit, Aktionen auf mehrere markierte Ereignisse auszuführen. Um mehrere Ereignisse zu markieren, halten Sie die **Strg**-**Taste** oder die **Shift-Taste** (Auswahl untereinander stehender Ereignisse) gedrückt, während Sie die Ereignisse auswählen. Um alle angezeigten Ereignisse auszuwählen, drücken Sie **Strg + A**.
> Bei der Aktion **Ausgewähltes Ereignis anzeigen** ist die Ausführung auf eine mehrfache Objektauswahl nicht möglich.

Module

Die Ereignisse folgender Module (hier in alphabetischer Reihenfolge) können mit Hilfe der Ereignisanzeige dargestellt werden:

Module's name
Hilfsdienst
Email-Schutz
Echtzeit-Scanner
Planer
System-Scanner
Updater
Browser-Schutz
ProActiv

Durch Markieren des Kontrollkästchens **Alle** können Sie sich die Ereignisse aller verfügbaren Module anzeigen lassen. Um sich nur die Ereignisse eines bestimmten Moduls anzeigen zu lassen, markieren Sie bitte das Kontrollkästchen vor dem gewünschten Modul.

Filter

In der Ereignisanzeige werden diese Ereignistypen angezeigt:

Symbol	Beschreibung
	Information
	Warnung
	Fehler
	Meldung

Durch Markieren des Kontrollkästchens **Filter** können Sie sich alle Ereignisse anzeigen lassen. Um sich nur bestimmte Ereignisse anzeigen zu lassen, markieren Sie bitte das Kontrollkästchen neben dem gewünschten Ereignis.

Tabelle

Die Ereignisanzeige enthält folgende Informationen:

- **Symbol**

  Das Symbol zur Darstellung des Ereignistyps.

- **Typ**

  Eine Klassifikation des Ereignisses: *Information*, *Warnung*, *Fehler*, *Fund*.

- **Modul**

  Das Avira Modul, das dieses Ereignis aufgezeichnet hat. Zum Beispiel der Echtzeit-Scanner, der einen Fund festgestellt hat.

- **Aktion**

  Ereignisbeschreibung des jeweiligen Moduls.

- **Datum/Uhrzeit**

  Datum und lokale Uhrzeit, wann das Ereignis aufgetreten ist.

7.3.15 Aktualisieren

Aktualisiert die Ansicht der geöffneten Rubrik.

7.4 Extras

7.4.1 Bootsektoren prüfen

Auch die Bootsektoren der Laufwerke Ihres Computers können Sie mit einer Direktsuche prüfen. Dies empfiehlt sich, wenn bei einer Direktsuche ein Virus gefunden wurde und Sie nun sicherstellen wollen, dass die Bootsektoren nicht betroffen sind.

Eine Auswahl mehrere Bootsektoren ist möglich, indem Sie die Shift-Taste (Hochstelltaste) gedrückt halten und mit der Maus die gewünschten Laufwerke auswählen.

> **Hinweis**
> Sie können die Bootsektoren bei jeder Direktsuche automatisch prüfen lassen (siehe Bootsektor Suchlaufwerke).

> **Hinweis**
> Unter Windows Vista ist das Prüfen der Bootsektoren nur mit Administratorrechten möglich.

7.4.2 Erkennungsliste

Mit dieser Funktion werden die Namen der Viren und unerwünschten Programme aufgelistet, die von Ihrem Avira Produkt erkannt werden können. Eine komfortable Suchfunktion für die Namen ist integriert.

Erkennungsliste durchsuchen

Geben Sie im Feld *Suchen nach:* einen Suchbegriff oder eine Zeichenfolge ein.

Suche nach Zeichenfolge innerhalb eines Namens

Sie können hier eine zusammenhängende Buchstaben- oder Zeichenfolge auf der Tastatur eingeben, die Markierung springt auf die erste Stelle auf der Namensliste, an der diese Zeichenfolge - auch mitten in einem Namen - steht (Beispiel: "raxa" findet "Abraxas").

Suche ab dem ersten Zeichen eines Namens

Sie können hier den Anfangsbuchstaben und die folgenden Zeichen auf der Tastatur eingeben, die Markierung blättert alphabetisch in der Namensliste (Beispiel: "Ra" findet "Rabbit").

Ist der gesuchte Name bzw. die Zeichenfolge vorhanden, wird die Fundstelle in der Liste markiert.

Suche vorwärts

Startet die Suche vorwärts in alphabetischer Reihenfolge.

Suche zurück

Startet die Suche rückwärts in alphabetischer Reihenfolge.

Erste Fundstelle

Springt in der Liste zum zuerst gefundenen Eintrag zurück.

Einträge in der Erkennungsliste

Unter diesem Titel befindet sich eine Liste mit Namen der Viren oder unerwünschten Programme, die erkannt werden können. Die meisten Einträge dieser Liste lassen sich auch mit Ihrem Avira Produkt entfernen. Sie sind jeweils alphabetisch geordnet (zuerst Sonderzeichen und Zahlen, dann die Buchstaben). Benutzen Sie die Bildlaufleiste, um in der Liste weiter nach unten oder zurück nach oben zu gelangen.

7.4.3 Rescue-CD herunterladen

Mit dem Menübefehl **Rescue-CD herunterladen** starten Sie einen Download des Avira Rescue-CD-Pakets. Das Paket beinhaltet ein bootfähiges Live-System für PCs sowie einen Avira Antiviren-Scanner mit aktuellster Virendefinitionsdatei und Suchengine. Sie nutzen die Avira Notfall-CD, um im Fall eines beschädigten Betriebssystems Ihren PC von der CD oder DVD aus zu starten und zu bedienen, um Daten zu retten oder eine Suche nach Viren und Malware durchzuführen.

Nach dem Download des Avira Rescue-CD-Pakets erscheint ein Dialogfenster, in dem Sie ein CD/DVD-Laufwerk auswählen, um die Rescue-CD zu brennen. Sie haben auch die Möglichkeit, das Avira Rescue-CD-Paket zu speichern, um die Notfall-CD zu einem späteren Zeitpunkt zu brennen.

> **Hinweis**
> Sie benötigen eine aktive Internetverbindung zum Download des Avira Rescue-CD-Pakets. Sie benötigen ein CD-/DVD-Laufwerk und eine beschreibbare CD oder DVD zum Brennen der Notfall-CD.

7.4.4 Konfiguration

Der Menüpunkt **Konfiguration** im Menü **Extras** öffnet die Konfiguration.

7.5 Update

7.5.1 Update starten...

Der Menüpunkt **Update starten...** im Menü **Update** startet ein Sofort-Update. Die Virendefinitionsdatei und die Suchengine werden aktualisiert. Ein Produktupdate erfolgt nur dann, wenn Sie in der Konfiguration unter PC Sicherheit > Update > Produktupdate die Option **Produktupdates herunterladen und automatisch installieren** aktiviert haben.

7.5.2 Manuelles Update...

Der Menüpunkt **Manuelles Update...** im Menü **Update** öffnet ein Dialogfenster zum Wählen und Laden eines VDF-/Engine-Update-Pakets. Das Update-Paket kann von der Webseite des Herstellers heruntergeladen werden und enthält die aktuelle Virendefinitionsdatei und Suchengine:
http://www.avira.de

> **Hinweis**
> Ab Windows Vista ist ein manuelles Update nur mit Administratorrechten möglich.

7.6 Hilfe

7.6.1 Inhalte

Der Menüpunkt **Inhalte** im Menü **Hilfe** öffnet das Inhaltsverzeichnis der Online-Hilfe.

7.6.2 Hilf mir

Der Menüpunkt **Hilf mir** im Menü **Hilfe** öffnet bei aktiver Internetverbindung die für Ihr Produkt relevante Support-Seite auf der Avira Webseite. Dort können Sie die Antworten zu den häufig gestellten Fragen lesen, die Wissensdatenbank abrufen oder den Avira Kundenservice kontaktieren.

7.6.3 Live Support

Der Menübefehl **Live Support** im Menü **Hilfe** öffnet bei aktiver Internetverbindung die Avira Webseite. Bitte laden Sie das Tool Avira Support Kundenmodul herunter. Das Kundenmodul wird für eine Remoteverbindung mit dem Avira Support benötigt. Kontaktieren Sie nach dem Download und der Installation des Moduls den Avira Support telefonisch, um Ihre Modul-ID mitzuteilen und einen Fernwartungstermin zu vereinbaren.

7.6.4 Forum

Der Menüpunkt **Forum** im Menü **Hilfe** öffnet bei aktiver Internetverbindung eine Webseite, über die Sie Zugriff auf das Avira Forum haben.

7.6.5 Download Handbuch

Der Menüpunkt **Download Handbuch** im Menü **Hilfe** öffnet bei aktiver Internetverbindung die Download-Seite von Ihrem Avira Produkt. Hier finden Sie den Link zum Download des aktuellsten Handbuchs zu Ihrem Avira Produkt.

7.6.6 Lizenzmanagement

Der Menüpunkt **Lizenzmanagement** im Menü **Hilfe** öffnet den Lizenz-Assistenten. Dieser Assistent hilft Ihnen, Ihr Avira Produkt auf einfache Art und Weise zu lizenzieren bzw. zu aktivieren.

Produkt aktivieren

Aktivieren Sie diese Option, wenn Sie bereits im Besitz eines Aktivierungscodes sind und das Avira Produkt noch nicht aktiviert haben. Bei der Produktaktivierung werden Sie als Kunde registriert, das Avira Produkt wird mit Ihrer Lizenz aktiviert. Den Aktivierungscode haben Sie entweder per Email von uns erhalten oder er ist auf der Produktverpackung vermerkt.

Hinweis
Die Aktivierung des Programms kann mit einem gültigen Aktivierungscode wiederholt ausgeführt werden, falls dies durch eine Neuinstallation des Systems erforderlich sein sollte.

Hinweis
Zur Produktaktivierung kommuniziert das Programm über das HTTP-Protokoll und Port 80 (Web-Kommunikation) sowie über das Verschlüsselungsprotokoll SSL und Port 443 mit den Avira Servern. Falls Sie eine Firewall nutzen, stellen Sie sicher, dass die benötigten Verbindungen und eingehende oder ausgehende Daten nicht von der Firewall blockiert werden.

Hinweis
Sie haben die Möglichkeit ein Produktupgrade auf ein Produkt aus der Avira Desktop-Produktfamilie anzustoßen (siehe Lizenzierung und Upgrade). Geben Sie den Aktivierungscode des Produkts, auf das Sie umsteigen möchten, im Eingabefeld Aktivierungscode ein. Falls das Upgrade möglich ist, erfolgt eine automatische Installation des Produkts.

Lizenz kaufen/verlängern

Diese Option wird angezeigt, wenn Ihre Lizenz abgelaufen, noch gültig ist oder Sie nur über eine Evaluationslizenz verfügen. Nutzen Sie die Option für eine Verlängerung Ihrer Produktlizenz oder den Erwerb einer Volllizenz.. Sie benötigen hierfür eine aktive Internetverbindung: Aktivieren Sie die Option *Lizenz kaufen/verlängern* und klicken Sie **Weiter**. Ihr Internetbrowser wird geöffnet, sie gelangen zum Avira Onlineshop, wo Sie eine Lizenz erwerben können.

Gültige Lizenzdatei

Über den Link **Lizenzdatei** können Sie eine gültige Lizenzdatei einlesen.
Die Lizenzdatei wird beim Vorgang der Produktaktivierung mit einem gültigen Aktivierungscode generiert, im Programmverzeichnis Ihres Avira Produkts gespeichert und eingelesen. Nutzen Sie die Option, wenn Sie eine Produktaktivierung bereits durchgeführt haben.

Proxy Einstellungen...

Bei Klick auf die Schaltfläche öffnet sich ein Dialogfenster. Bei Bedarf können Sie hier einstellen, dass Sie die Internetverbindung, die zur Produktaktivierung genutzt wird, über einen Proxyserver herstellen wollen.

7.6.7 Produkt empfehlen

Der Menübefehl **Produkt empfehlen** im Menü **Hilfe** öffnet bei aktiver Internetverbindung eine Webseite für Avira Kunden. Dort können Sie Ihr Avira Produkt weiterempfehlen und so an den Avira Rabattaktionen teilnehmen.

7.6.8 Feedback senden

Der Menübefehl **Feedback senden** im Menü **Hilfe** öffnet bei aktiver Internetverbindung eine Feedback-Seite zu den Avira Produkten. Dort finden Sie ein Formular zur Produktevaluierung, das Sie mit Ihren Angaben zur Produktqualität und weiteren Anregungen zum Produkt an Avira senden können.

7.6.9 Über Avira Antivirus Suite

Allgemein

Adressen und Informationen zu Ihrem Avira Produkt

Versionsinformationen

Versionsinformationen zu Dateien innerhalb des Avira Produktpakets

Lizenzinformationen

Lizenzdaten der aktuellen Lizenz und Links zum Onlineshop (Erwerb oder die Verlängerung einer Lizenz)

> **Hinweis**
> Sie können die Lizenzdaten im Zwischenspeicher ablegen. Klicken Sie mit der rechten Maustaste in den Bereich Lizenzdaten. Es öffnet sich ein Kontextmenü. Klicken Sie in dem Kontextmenü auf den Menübefehl **In Zwischenablage** kopieren. Ihre Lizenzdaten sind nun in der Zwischenablage gespeichert und können über den Windows Befehl zum Einfügen in Emails, Formulare oder Dokumente eingefügt werden.

7.7 Experts Market

7.7.1 Experts Market Überblick

Bei Experts Market handelt es sich um eine Datenbank, die einerseits Anwendern dabei hilft, Experten zu kontaktieren, die ihnen bei Computerproblemen mit Rat und Tat zur Seite stehen, und es andererseits Experten ermöglicht, für Anwender, die ihrer Hilfe bedürfen, leicht erreichbar zu sein.

In den folgenden Kapiteln finden Sie Informationen, wie Sie

Hilfe anfordern
Hilfe anbieten

7.7.2 Hilfe anfordern

Wir haben es uns zum Ziel gesetzt, unser Produkt so verständlich und benutzerfreundlich wie möglich zu entwickeln. Manchmal ergeben sich jedoch Fragen und Situationen, in denen Sie sich nicht sicher sind, wie Sie damit umgehen sollen und die Hilfe eines Experten begrüßen würden. Mithilfe von Avira Antivirus Suite können Sie aus einer Datenbank Einzelpersonen und Firmen heraussuchen, die Ihnen dabei helfen, Ihre Computer- und Software-Probleme zu beheben.

- Starten Sie Avira Antivirus Suite.

  Klicken Sie **Avira Experts Market besuchen**.

  ↬ Sie werden auf die Avira Experts Market Webseite weitergeleitet.

- Klicken Sie **Experten finden**.

  ↬ Sie werden zur Experten-Datenbank weitergeleitet, wo Sie eine Ihren Wünschen entsprechende Suchanfrage ausführen können.

Das Profil eines jeden Experten beinhaltet folgende Informationen:

- *Profilbild*
- *Expertenname*
- *Stadt*
- *Land*
- *Verfügbarkeit*
- *Beschreibung*
- *Benutzerbewertung*
- *Zufriedene Kunden*
- *Fachkenntnisse*
- *Preisinformationen*

Die Experten können nach **Benutzerbewertung** oder der Anzahl **Zufriedener Kunden** sortiert werden.

- Um auf der Stelle mit einem Experten in Kontakt zu treten, klicken Sie **Jetzt chatten**.

  ↬ Ein Chatfenster öffnet sich, in dem Sie direkt mit Ihrem Experten darüber verhandeln können, wie Sie vorgehen möchten.

- Wenn der ausgewählte Experte offline oder beschäftigt ist, klicken Sie **Nachricht senden** .

↳ Ein Email-Formular öffnet sich, mit dessen Hilfe Sie eine Email an den Experten schicken können.

7.7.3 Hilfe anbieten

Wenn Sie ein erfahrender Anwender sind, für den Computerprobleme kein Problem darstellen und Sie gerne anderen Avira Anwendern helfen würden, können Sie sich als Experte registrieren. Die Registrierung ist sowohl Einzelpersonen als auch Unternehmen möglich.

- Starten Sie Avira Antivirus Suite.

  Klicken Sie **Avira Experts Market** besuchen.

  ↳ Sie werden auf die Avira Experts Market Webseite weitergeleitet.

- Klicken Sie **Erfahren Sie mehr**.

  ↳ Ein Registrierungsformular wird angezeigt.

- Tragen Sie die erforderlichen Informationen ein und klicken Sie **Registrieren**.

  ↳ Eine Bestätigungsnachricht wird angezeigt und eine Email mit einem Aktivierungslink an Ihre Email-Adresse gesendet.

- Klicken Sie den Aktivierungslink.

  ↳ EIne Webseite mit den Geschäftsbedingungen öffnet sich.

- Geben Sie ein Passwort für Ihr Experten-Konto ein und klicken Sie **Aktivieren**.

  Wenn die Bestätigungsnachricht angezeigt wird, klicken Sie **Zum Expertenportal**.

  Nun können Sie damit beginnen, anderen Anwendern zu helfen.

Die erforderlichen Informationen für Ihre Registrierung beinhalten folgendes:

- Experte
- Anrede
- Vorname
- Nachname
- Email-Adresse
- Straße
- Postleitzahl
- Land

Sie können außerdem folgende Informationen angeben:

- Staat/Bundesland
- Telefonnummer
- Faxnummer

- Firmenname
- Handelsregisternummer
- Steuernummer
- Webseite

8. Kinderschutz

Nutzen Sie Aviras *KINDERSCHUTZ* Funktionen, um ein sicheres Internet-Erlebnis für Ihre Kinder oder andere Personen, die Ihren Rechner benutzen, zu ermöglichen.

- Die Rubrik **Soziale Netzwerke** leitet Sie zur Avira Kinderschutz für soziale Netzwerke Anwendung weiter. Avira Kinderschutz für soziale Netzwerke informiert Eltern über die Online-Aktivitäten ihrer Kinder. Das System prüft die Konten der sozialen Netzwerke auf Kommentare, Fotos usw., die dem Ruf ihres Kindes schaden könnten oder die darauf hinweisen könnten, dass Ihr Kind gefährdet ist.

Verwandte Themen:

- Soziale Netzwerke

8.1 Soziale Netzwerke

Dieses Kapitel enthält umfassende Informationen über

Ein Kinderschutz-Konto für Soziale Netzwerke erstellen
Mit einem bestehenden Kinderschutz-Konto für Soziale Netzwerke anmelden

8.1.1 Ein Konto für Soziale Netzwerke erstellen

- Vergewissern Sie sich, dass Ihr Computer mit dem Internet verbunden ist.

  Klicken Sie **Control Center > Ansicht > Kinder Schutz > Soziale Netzwerke**.

  Klicken Sie **Starten Sie jetzt**.

  ↳ Der Webbrowser öffnet die Webseite des Avira Kinderschutz für Soziale Netzwerke.

- Falls Sie einen Facebook Account besitzen, können Sie sich jetzt bei Ihrem Kinderschutz-Konto für Soziale Netzwerke anmelden, indem Sie das Facebook-Logo anklicken.

-ODER-

- Falls Sie keinen Facebook Account besitzen, geben Sie Ihren Vornamen, Ihren Nachnamen, Ihre Email-Adresse und ein Passwort in die entsprechenden Felder ein und klicken Sie **Starten Sie jetzt**.

> **Hinweis**
> Ab jetzt fungiert Ihre Email-Adresse als Ihr Benutzername.

8.1.2 Mit einem bestehenden Kinderschutz-Konto für Soziale Netzwerke anmelden

- Vergewissern Sie sich, dass Ihr Computer mit dem Internet verbunden ist.
- Klicken Sie **Control Center > Ansicht > Kinderschutz > Soziale Netzwerke**.

  Klicken Sie **Anmelden**.

  ↳ Wenn Sie den Cookie auf Ihrem System gespeichert haben, öffnet sich Ihr Webbrowser und zeigt sofort den Aktivitätsmonitor Ihres Avira Kinderschutz für Soziale Netzwerke an.

-ODER-

↳ Wenn Ihr Webbrowser keine Cookies speichert oder sie bei jedem Schließen des Webbrowsers löscht, können Sie sich anmelden, indem Sie entweder auf das **Facebook Logo** klicken oder Ihren Benutzernamen und Passwort eingeben.

9. Mobiler Schutz

Avira schützt nicht nur Ihren Computer vor Malware und Viren, wir schützen auch Smartphones, die mit dem Betriebssystem Android arbeiten, vor Diebstahl und/oder Verlust. Mithilfe der Avira Android Security Blockierliste können Sie desweiteren unerwünschte Anrufe und SMS fernhalten. Fügen Sie einfach Telefonnummern aus Ihrer Anruferliste, der Nachrichtenliste oder Ihren Kontakten zur Blockierliste hinzu, oder erstellen Sie manuell Kontakte, die Sie blockieren möchten.

Weitere Informationen finden Sie auf unserer Webseite:

www.avira.de/android

10. Konfiguration

10.1 Konfigurationsoptionen im Überblick

Sie haben folgende Konfigurationsoptionen:

- **System-Scanner**: Konfiguration der Direktsuche
  - Suchoptionen
  - Aktion bei Fund
  - Optionen bei Suche in Archiven
  - Ausnahmen der Direktsuche
  - Heuristik der Direktsuche
  - Einstellung der Reportfunktion
- **Echtzeit-Scanner**: Konfiguration der Echtzeitsuche
  - Suchoptionen
  - Aktion bei Fund
  - Weitere Aktionen
  - Ausnahmen der Echtzeitsuche
  - Heuristik der Echtzeitsuche
  - Einstellung der Reportfunktion
- **Update**: Konfigurationen der Update-Einstellungen, Einstellung der Produktupdates
  - Download über Webserver
  - Proxy Einstellungen
- **Browser-Schutz**: Konfiguration des Browser-Schutzes
  - Suchoptionen, Aktivierung und Deaktivierung des Browser-Schutzes
  - Aktion bei Fund
  - Gesperrte Zugriffe: Unerwünschte Dateitypen und MIME-Typen, Web-Filter für bekannte unerwünschte URLS (Malware, Phishing etc.)
  - Ausnahmen der Suche des Browser-Schutzes: URLs, Dateitypen, MIME-Typen
  - Heuristik des Browser-Schutzes
  - Einstellung der Reportfunktion
- **Email-Schutz**: Konfiguration des Email-Schutzes
  - Suchoptionen: Aktivierung der Überwachung von POP3-Konten, IMAP-Konten, ausgehenden Emails (SMTP)

- Aktion bei Fund
- Weitere Aktionen
- Heuristik der Suche des Email-Schutzes
- AntiBot-Funktion: Erlaubte SMTP-Server, erlaubte Email-Absender
- Ausnahmen der Suche des Email-Schutzes
- Konfiguration des Zwischenspeichers, Zwischenspeicher leeren
- Einstellung der Reportfunktion

- **Allgemeines**:
  - Erweiterte Gefahrenkategorien für Direkt- und Echtzeitsuche
  - Anwendungsfilter: Anwendungen blockieren oder erlauben
  - Erweiterter Schutz: Optionen, um ProActiv und Cloud-Sicherheit zu aktivieren.
  - Kennwortschutz für den Zugriff auf das Control Center und die Konfiguration
  - Sicherheit: Autorun Funktionen blockieren, Windows hosts-Datei sperren, Produktschutz
  - WMI: WMI-Unterstützung aktivieren
  - Konfiguration der Ereignis-Protokollierung
  - Konfiguration der Bericht-Funktionen
  - Einstellung der verwendeten Verzeichnisse
  - Konfiguration von akustischen Warnungen bei Malware-Fund

10.1.1 Schaltflächen

Schaltfläche	Beschreibung
Standardwerte	Alle Einstellungen in der Konfiguration werden auf Standardwerte zurückgesetzt. Alle Änderungen und alle eigenen Einträge gehen beim Zurücksetzen auf die Standardwerte verloren.
OK	Alle vorgenommenen Einstellungen werden gespeichert. Die Konfiguration wird geschlossen. Die Benutzerkontensteuerung (UAC) benötigt Ihre Zustimmung um die vorgenommenen Änderungen in Betriebssystemen ab Windows Vista zu übernehmen.
Abbrechen	Die Konfiguration wird geschlossen ohne Ihre vorgenommenen Einstellungen in der Konfiguration zu speichern.
Übernehmen	Alle vorgenommenen Einstellungen werden gespeichert. Die Benutzerkontensteuerung (UAC) benötigt Ihre Zustimmung um die vorgenommenen Änderungen in Betriebssystemen ab Windows Vista zu übernehmen.

10.2 System-Scanner

Die Rubrik **System-Scanner** der Konfiguration ist für die Konfiguration der Direktsuche, d.h. für die Suche auf Verlangen, zuständig. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

10.2.1 Suche

Sie können hier das grundlegende Verhalten der Suchroutine bei einer Direktsuche festlegen. Wenn Sie bei der Direktsuche bestimmte Verzeichnisse für die Prüfung wählen, prüft der System-Scanner je nach Konfiguration:

- mit einer bestimmten Suchleistung (Priorität),
- zusätzlich Bootsektoren und Hauptspeicher,
- alle oder ausgewählte Dateien im Verzeichnis.

Dateien

Der System-Scanner kann einen Filter verwenden, um nur Dateien mit einer bestimmten Endung (Typ) zu prüfen.

Alle Dateien

Bei aktivierter Option werden alle Dateien, unabhängig von ihrem Inhalt und ihrer Dateierweiterung, nach Viren bzw. unerwünschten Programmen durchsucht. Der Filter wird nicht verwendet.

> **Hinweis**
> Ist **Alle Dateien** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch vom Programm übernommen. D.h. Ihr Avira Produkt entscheidet anhand des Inhalts einer Datei, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht. Dieses Verfahren ist etwas langsamer als Dateierweiterungsliste verwenden, aber wesentlich sicherer, da nicht nur anhand der Dateierweiterung geprüft wird. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

> **Hinweis**
> Ist **Intelligente Dateiauswahl** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Dateierweiterungsliste verwenden

Bei aktivierter Option werden nur Dateien mit einer vorgegebenen Endung durchsucht. Voreingestellt sind alle Dateitypen, die Viren und unerwünschte Programme enthalten können. Die Liste lässt sich über die Schaltfläche "**Dateierweiterungen"** manuell editieren.

> **Hinweis**
> Ist diese Option aktiv und Sie haben alle Einträge aus der Liste mit Dateiendungen gelöscht, wird dies durch den Text "*Keine Dateierweiterungen*" unterhalb der Schaltfläche **Dateierweiterungen** angezeigt.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Suchlauf im Modus "**Dateierweiterungsliste verwenden"** untersucht werden. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.

> **Hinweis**
> Beachten Sie bitte, dass sich die Standardliste von Version zu Version ändern kann.

Weitere Einstellungen

Bootsektor Suchlaufwerke

Bei aktivierter Option prüft der System-Scanner die Bootsektoren der bei der Direktsuche gewählten Laufwerke. Diese Einstellung ist standardmäßig aktiviert.

Masterbootsektoren durchsuchen

Bei aktivierter Option prüft der System-Scanner die Masterbootsektoren der im System verwendeten Festplatte(n).

Offline Dateien ignorieren

Bei aktivierter Option ignoriert die Direktsuche sog. Offline Dateien bei einem Suchlauf komplett. D.h., diese Dateien werden nicht auf Viren und unerwünschte Programme geprüft. Offline Dateien sind Dateien, die durch ein sog. Hierarchisches Speicher-Management-System (HSMS) physikalisch von der Festplatte auf z.B. ein Band ausgelagert wurden. Diese Einstellung ist standardmäßig aktiviert.

Integritätsprüfung von Systemdateien

Bei aktivierter Option werden bei jeder Direktsuche die wichtigsten Windows Systemdateien einer besonders sicheren Prüfung auf Veränderungen durch Malware unterzogen. Wird eine veränderte Datei gefunden, wird diese als verdächtiger Fund



gemeldet. Die Funktion nimmt viel Rechnerleistung in Anspruch. Daher ist die Option standardmäßig deaktiviert.

Hinweis
Die Option ist nur ab Windows Vista verfügbar.

Hinweis
Falls Sie Drittanbieter Tools einsetzen, die Systemdateien verändern und den Boot- oder Startbildschirm auf eigene Bedürfnisse anpassen, sollten Sie diese Option nicht verwenden. Beispiele für diese Tools sind sogenannte Skinpacks, TuneUp Utilities oder Vista Customization.

Optimierter Suchlauf

Bei aktivierter Option wird die Prozessor-Kapazität bei einem Suchlauf des System-Scanners optimal ausgelastet. Aus Gründen der Performance erfolgt die Protokollierung beim optimierten Suchlauf höchstens auf einem Standard-Level.

Hinweis
Die Option ist nur bei Multi-Prozessor-Rechnern verfügbar.

Symbolischen Verknüpfungen folgen

Bei aktivierter Option folgt der System-Scanner bei einer Suche allen symbolischen Verknüpfungen im Suchprofil oder ausgewählten Verzeichnis, um die verknüpften Dateien nach Viren und Malware zu durchsuchen.

Hinweis
Die Option schließt keine Dateiverknüpfungen (Shortcuts) ein, sondern bezieht sich ausschließlich auf symbolische Links (erzeugt mit mklink.exe) oder Junction Points (erzeugt mit junction.exe), die transparent im Dateisystem vorliegen.

Rootkits-Suche bei Suchstart

Bei aktivierter Option prüft der System-Scanner bei einem Suchstart in einem sog. Schnellverfahren das Windows-Systemverzeichnis auf aktive Rootkits. Dieses Verfahren prüft Ihren Rechner nicht so umfassend auf aktive Rootkits wie das Suchprofil "**Suche nach Rootkits"**, ist jedoch in der Ausführung bedeutend schneller. Diese Option ändert nur die Einstellungen der von Ihnen selbst erstellten Profile.

Hinweis
Die Rootkits-Suche ist unter Windows XP 64 Bit nicht verfügbar!

Registry durchsuchen

Bei aktivierter Option wird bei einem Suchlauf die Registry nach Verweisen auf Schadsoftware durchsucht. Diese Option ändert nur die Einstellungen der von Ihnen selbst erstellten Profile.

Dateien und Pfade auf Netzlaufwerken ignorieren

Bei aktivierter Option sind mit dem Computer verbundene Netzlaufwerke von der Direktsuche ausgenommen. Diese Option empfiehlt sich, wenn die Server oder andere Workstations selbst durch eine Antiviren-Software geschützt werden. Diese Option ist standardmäßig deaktiviert.

Suchvorgang

Stoppen zulassen

Bei aktivierter Option, lässt sich die Suche nach Viren oder unerwünschten Programmen jederzeit mit der Schaltfläche "**Stopp"** im Fenster "Luke Filewalker" beenden. Haben Sie diese Einstellung deaktiviert, wird die Schaltfläche **Stopp** im Fenster "Luke Filewalker" grau unterlegt. Das vorzeitige Beenden eines Suchlaufs ist so nicht möglich! Diese Einstellung ist standardmäßig aktiviert.

Scanner-Priorität

Der System-Scanner unterscheidet bei der Direktsuche drei Prioritätsstufen. Dies ist nur wirksam, wenn auf dem Computer mehrere Prozesse gleichzeitig ablaufen. Die Wahl wirkt sich auf die Suchgeschwindigkeit aus.

niedrig

Der System-Scanner erhält vom Betriebssystem nur dann Prozessorzeit zugewiesen, wenn kein anderer Prozess Rechenzeit benötigt, d.h. solange der System-Scanner alleine läuft, ist die Geschwindigkeit maximal. Insgesamt wird die Arbeit mit anderen Programmen dadurch sehr gut ermöglicht: Der Computer reagiert schneller, wenn andere Programme Rechenzeit benötigen, während dann der System-Scanner im Hintergrund weiterläuft.

mittel

Der System-Scanner wird mit normaler Priorität ausgeführt. Alle Prozesse erhalten vom Betriebssystem gleich viel Prozessorzeit zugewiesen. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen. Unter Umständen ist die Arbeit mit anderen Anwendungen beeinträchtigt.



hoch

Der System-Scanner erhält höchste Priorität. Ein paralleles Arbeiten mit anderen Anwendungen ist kaum mehr möglich. Jedoch erledigt der System-Scanner seinen Suchlauf maximal schnell.

Aktion bei Fund

Sie können Aktionen festlegen, die der System-Scanner ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde.

Interaktiv

Bei aktivierter Option werden Funde der Suche des System-Scanners in einem Dialogfenster gemeldet. Bei der Suche des System-Scanners erhalten Sie beim Abschluss des Suchlaufs eine Warnmeldung mit einer Liste der gefundenen betroffenen Dateien. Sie haben die Möglichkeit, über das Kontextmenü eine auszuführende Aktion für die einzelnen betroffenen Dateien auszuwählen. Sie können die gewählten Aktionen für alle betroffenen Dateien ausführen oder den System-Scanner beenden.

> **Hinweis**
> Standardmäßig ist im Dialogfenster zur Virenbehandlung die Aktion **Quarantäne** vorausgewählt. Über ein Kontextmenü können Sie weitere Aktionen auswählen.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der System-Scanner reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Datei vor Aktion in Quarantäne kopieren

Bei aktivierter Option erstellt der System-Scanner eine Sicherheitskopie (Backup) vor der Durchführung der gewünschten primären bzw. sekundären Aktion. Die Sicherheitskopie wird in der Quarantäne aufbewahrt, wo die Datei wiederhergestellt werden kann, wenn sie einen informativen Wert hat. Zudem können Sie die Sicherheitskopie für weitere Untersuchungen an das Avira Malware Research Center senden.

Primäre Aktion

Primäre Aktion, ist die Aktion die ausgeführt wird, wenn der System-Scanner einen Virus bzw. ein unerwünschtes Programm findet. Ist die Option "**Reparieren"** gewählt, jedoch eine Reparatur der betroffenen Datei nicht möglich, wird die unter "**Sekundäre Aktion"** gewählte Aktion ausgeführt.

Hinweis
Die Option **Sekundäre Aktion** ist nur dann auswählbar, wenn unter **Primäre Aktion** die Einstellung **Reparieren** ausgewählt wurde.

Reparieren

Bei aktivierter Option repariert der System-Scanner betroffene Dateien automatisch. Wenn der System-Scanner eine betroffene Datei nicht reparieren kann, führt er alternativ die unter Sekundäre Aktion gewählte Option aus.

Hinweis
Eine automatische Reparatur wird empfohlen, bedeutet aber, dass der System-Scanner Dateien auf dem Computer verändert.

Umbenennen

Bei aktivierter Option benennt der System-Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Die Datei kann später repariert und zurück benannt werden.

Quarantäne

Bei aktivierter Option verschiebt der System-Scanner die Datei in Quarantäne. Diese Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

Ignorieren

Bei aktivierter Option wird die Datei belassen.

Warnung Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Überschreiben und löschen

Bei aktivierter Option überschreibt der System-Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Sekundäre Aktion

Die Option "**Sekundäre Aktion"** ist nur dann auswählbar, wenn unter "**Primäre Aktion"** die Einstellung **Reparieren** ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was mit der betroffenen Datei geschehen soll, wenn diese nicht reparabel ist.



Umbenennen

Bei aktivierter Option benennt der System-Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Die Datei kann später repariert und zurück benannt werden.

Quarantäne

Bei aktivierter Option verschiebt der System-Scanner die Datei in Quarantäne. Diese Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

Ignorieren

Bei aktivierter Option wird die Datei belassen.

Warnung Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Überschreiben und löschen

Bei aktivierter Option überschreibt der System-Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Hinweis
Wenn Sie als primäre oder sekundäre Aktion **Löschen** oder **Überschreiben und löschen** ausgewählt haben, beachten Sie bitte folgendes: Bei heuristischen Treffern werden die betroffenen Dateien nicht gelöscht, sondern in die Quarantäne verschoben.

Archive

Bei der Suche in Archiven wendet der System-Scanner eine rekursive Suche an: Es werden auch Archive in Archiven entpackt und auf Viren und unerwünschte Programme geprüft. Die Dateien werden geprüft, dekomprimiert und noch einmal geprüft. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Archive durchsuchen

Bei aktivierter Option werden die in der Archiv-Liste markierten Archive geprüft. Diese Einstellung ist standardmäßig aktiviert.

Alle Archiv-Typen

Bei aktivierter Option werden alle Archivtypen in der Archiv-Liste markiert und geprüft.

Smart Extensions

Bei aktivierter Option erkennt der System-Scanner, ob es sich bei einer Datei um ein gepacktes Dateiformat (Archiv) handelt, auch wenn die Dateiendung von den gebräuchlichen Endungen abweicht, und prüft das Archiv. Dafür muss jedoch jede Datei geöffnet werden - was die Suchgeschwindigkeit verringert. Beispiel: Wenn ein *.zip-Archiv mit der Dateiendung *.xyz versehen ist, entpackt der System-Scanner auch dieses Archiv und prüft es. Diese Einstellung ist standardmäßig aktiviert.

> **Hinweis**
> Es werden nur diejenigen Archivtypen geprüft, die in der Archiv-Liste markiert sind.

Rekursionstiefe einschränken

Das Entpacken und Prüfen bei sehr tief geschachtelten Archiven kann sehr viel Rechnerzeit und -Ressourcen benötigen. Bei aktivierter Option beschränken Sie die Tiefe der Suche in mehrfach gepackten Archiven auf eine bestimmte Zahl an Pack-Ebenen (Maximale Rekursionstiefe). So sparen Sie Zeit- und Rechnerressourcen.

> **Hinweis**
> Um einen Virus bzw. ein unerwünschtes Programm innerhalb eines Archivs zu ermitteln, muss der System-Scanner bis zu der Rekursions-Ebene scannen, in der sich der Virus bzw. das unerwünschte Programm befindet.

Maximale Rekursionstiefe

Um die maximale Rekursionstiefe eingeben zu können, muss die Option **Rekursionstiefe einschränken** aktiviert sein.
Sie können die gewünschte Rekursionstiefe entweder direkt eingeben oder aber mittels der Pfeiltasten rechts vom Eingabefeld ändern. Erlaubte Werte sind 1 bis 99. Der Standardwert ist 20 und wird empfohlen.

Standardwerte

Die Schaltfläche stellt die vordefinierten Werte für die Suche in Archiven wieder her.

Archiv-Liste

In diesem Anzeigebereich können Sie einstellen, welche Archive der System Scanner durchsuchen soll. Sie müssen hierfür die entsprechenden Einträge markieren.

Ausnahmen

Vom System-Scanner auszulassende Dateiobjekte (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Die Liste in diesem Fenster enthält Dateien und Pfade, die bei der Suche nach Viren bzw. unerwünschten Programmen vom System-Scanner nicht berücksichtigt werden sollen.

Bitte tragen Sie hier so wenige Ausnahmen wie möglich und wirklich nur Dateien ein, die aus welchen Gründen auch immer, bei einem normalen Suchlauf nicht geprüft werden sollen. Wir empfehlen, diese Dateien auf jeden Fall auf Viren bzw. unerwünschte Programme zu untersuchen, bevor sie in diese Liste aufgenommen werden!

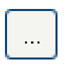
Hinweis
Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

Warnung
Diese Dateien werden bei einem Suchlauf nicht berücksichtigt!

Hinweis
Die in dieser Liste aufgenommenen Dateien werden in der Reportdatei vermerkt. Kontrollieren Sie bitte von Zeit zu Zeit die Reportdatei nach diesen nicht überprüften Dateien, denn vielleicht gibt es den Grund, aus dem Sie eine Datei hier ausgenommen haben gar nicht mehr. Dann sollten Sie den Namen dieser Datei aus der Liste wieder entfernen.

Eingabefeld

In dieses Feld geben Sie den Namen des Dateiobjekts ein, der von der Direktsuche nicht berücksichtigt wird. Standardmäßig ist kein Dateiobjekt eingegeben.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei bzw. den gewünschten Pfad auszuwählen.
Haben Sie einen Dateinamen mit vollständigem Pfad eingegeben, wird genau diese Datei nicht auf Befall überprüft. Falls Sie einen Dateinamen ohne Pfad eingetragen haben, wird jede Datei mit diesem Namen (egal in welchem Pfad oder auf welchem Laufwerk) nicht durchsucht.

Hinzufügen

Mit der Schaltfläche können Sie das im Eingabefeld eingegebene Dateiobjekt in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD aktivieren

Ihr Avira Programm beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

10.2.2 Report

Der System-Scanner besitzt eine umfangreiche Protokollierfunktion. Damit erhalten Sie exakte Informationen über die Ergebnisse einer Direktsuche. Die Reportdatei enthält alle Einträge des Systems sowie Warnungen und Meldungen der Direktsuche. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)



> **Hinweis**
> Damit Sie bei einem Fund von Viren oder unerwünschten Programmen nachvollziehen können, welche Aktionen der System-Scanner ausgeführt hat, sollte immer eine Reportdatei erstellt werden.

Protokollierung

Aus

Bei aktivierter Option protokolliert der System-Scanner die Aktionen und Ergebnisse der Direktsuche nicht.

Standard

Bei aktivierter Option protokolliert der System-Scanner die Namen der betroffenen Dateien mit Pfadangabe. Zudem wird die Konfiguration für den aktuellen Suchlauf, Versionsinformationen und Informationen zum Lizenznehmer in die Reportdatei geschrieben.

Erweitert

Bei aktivierter Option protokolliert der System-Scanner zusätzlich zu den Standard-Informationen auch Warnungen und Hinweise. Die Reportdatei zeigt ein "(Cloud)"-Suffix an, um die Warnungen von der Cloud-Sicherheit zu identifizieren.

Vollständig

Bei aktivierter Option protokolliert der System-Scanner zusätzlich alle durchsuchten Dateien. Zudem werden alle betroffenen Dateien sowie Warnungen und Hinweise mit in die Reportdatei aufgenommen.

> **Hinweis**
> Sollten Sie uns einmal eine Reportdatei zusenden müssen (zur Fehlersuche), bitten wir Sie, diese Reportdatei in diesem Modus zu erstellen.

10.3 Echtzeit-Scanner

Die Rubrik Echtzeit-Scanner der Konfiguration ist für die Konfiguration der Echtzeitsuche zuständig. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

10.3.1 Suche

Üblicherweise werden Sie Ihr System ständig überwachen wollen. Dafür nutzen Sie den Echtzeit-Scanner (Echtzeitsuche = On-Access-Scanner). Damit können Sie u.a. alle Dateien, die auf dem Computer kopiert oder geöffnet werden, "on the fly", nach Viren und unerwünschten Programmen durchsuchen lassen. (Option nur bei aktiviertem Expertenmodus verfügbar.)

Dateien

Der Echtzeit-Scanner kann einen Filter verwenden, um nur Dateien mit einer bestimmten Endung (Typ) zu prüfen.

Alle Dateien

Bei aktivierter Option werden alle Dateien, unabhängig von ihrem Inhalt und ihrer Dateierweiterung, nach Viren bzw. unerwünschten Programmen durchsucht.

> **Hinweis**
> Ist **Alle Dateien** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch vom Programm übernommen. Dies bedeutet, dass das Programm anhand des Inhalts einer Datei entscheidet, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht. Dieses Verfahren ist etwas langsamer als **Dateierweiterungsliste verwenden**, aber wesentlich sicherer, da nicht nur anhand der Dateierweiterung geprüft wird.

> **Hinweis**
> Ist **Intelligente Dateiauswahl** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Dateierweiterungsliste verwenden

Bei aktivierter Option werden nur Dateien mit einer vorgegebenen Endung durchsucht. Voreingestellt sind alle Dateitypen, die Viren und unerwünschte Programme enthalten können. Die Liste lässt sich über die Schaltfläche "**Dateierweiterung"** manuell editieren. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

> **Hinweis**
> Ist diese Option aktiv und Sie haben alle Einträge aus der Liste mit Dateiendungen gelöscht, wird dies durch den Text "*Keine Dateierweiterungen*" unterhalb der Schaltfläche **Dateierweiterungen** angezeigt.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Suchlauf im Modus "**Dateierweiterungsliste verwenden"** untersucht werden. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.

> **Hinweis**
> Beachten Sie bitte, dass sich die Dateierweiterungsliste von Version zu Version ändern kann.

Laufwerke

Netzwerklaufwerke überwachen

Bei aktivierter Option werden Dateien auf Netzlaufwerken (gemappte Laufwerke) wie z.B. Server-Volumes, Peer-Laufwerke, etc. überwacht.

> **Hinweis**
> Um die Leistungsfähigkeit Ihres Rechners nicht zu stark zu beeinträchtigen, sollte die Option **Netzwerklaufwerke überwachen** nur im Ausnahmefall aktiviert werden.

> **Warnung**
> Bei deaktivierter Option werden die Netzlaufwerke **nicht** überwacht. Sie sind nicht mehr vor Viren bzw. unerwünschten Programmen geschützt!

> **Hinweis**
> Wenn Dateien auf Netzlaufwerken ausgeführt werden, werden diese vom Echtzeit Scanner durchsucht - unabhängig von der Einstellung der Option **Netzwerklaufwerke überwachen**. In einigen Fällen werden Dateien auf Netzlaufwerken beim Öffnen durchsucht, obwohl die Option **Netzwerklaufwerke überwachen** deaktiviert ist. Der Grund: Auf diese Dateien wird mit der Berechtigung 'Datei ausführen' zugegriffen. Wenn Sie diese Dateien oder auch ausgeführte Dateien auf Netzlaufwerken von einer Überwachung des Echtzeit-Scanners ausnehmen wollen, tragen Sie die Dateien in die Liste der auszulassenden Dateiobjekte ein (siehe: Ausnahmen).

Caching aktivieren

Bei aktivierter Option werden überwachte Dateien auf Netzlaufwerken im Cache des Echtzeit-Scanners zur Verfügung gestellt. Die Überwachung von Netzlaufwerken ohne Caching-Funktion bietet mehr Sicherheit, ist jedoch weniger performant als die Überwachung von Netzlaufwerken mit Caching-Funktion.

Archive

Archive durchsuchen

Bei aktivierter Option werden Archive durchsucht. Die komprimierten Dateien werden durchsucht, dekomprimiert und noch einmal durchsucht. Standardmäßig ist die Option deaktiviert. Die Archivsuche wird über die Rekursionstiefe, die Anzahl der zu



durchsuchenden Dateien und die Archivgröße eingeschränkt. Sie können die maximale Rekursionstiefe, die Anzahl der zu durchsuchenden Dateien und die maximale Archivgröße einstellen.

> **Hinweis**
> Die Option ist standardmäßig deaktiviert, da der Prozess sehr viel Rechnerleistung in Anspruch nimmt. Generell wird empfohlen, Archive mit der Direktsuche zu prüfen.

Max. Rekursionstiefe

Bei der Suche in Archiven wendet der Echtzeit-Scanner eine rekursive Suche an: Es werden auch Archive in Archiven entpackt und auf Viren und unerwünschte Programme geprüft. Sie können die Rekursionstiefe festlegen. Der Standardwert für die Rekursionstiefe ist 1 und wird empfohlen: Alle Dateien, die direkt im Hauptarchiv liegen, werden durchsucht.

Max. Anzahl Dateien

Bei der Suche in Archiven wird die Suche auf eine maximale Anzahl von Dateien im Archiv beschränkt. Der Standardwert für die maximale Anzahl zu durchsuchender Dateien ist 10 und wird empfohlen.

Max. Größe (KB)

Bei der Suche in Archiven wird die Suche auf eine maximale, zu entpackende Archivgröße beschränkt. Der Standardwert ist 1000 KB und wird empfohlen.

Aktion bei Fund

Sie können Aktionen festlegen, die der Echtzeit-Scanner ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Interaktiv

Bei aktivierter Option erscheint bei einem Fund des Echtzeit-Scanners eine Desktop-Benachrichtigung. Sie haben die Möglichkeit, die gefundene Malware zu entfernen oder weitere mögliche Aktionen zur Virenbehandlung über die Schaltfläche "**Details**" abzurufen. Die Aktionen werden in einem Dialogfenster angezeigt. Diese Option ist standardmäßig aktiviert.

Reparieren

Der Echtzeit-Scanner repariert die betroffene Datei, falls dies möglich ist.

Umbenennen

Der Echtzeit-Scanner benennt die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Die Datei kann später repariert und wieder umbenannt werden.



Quarantäne

Der Echtzeit-Scanner verschiebt die Datei in die Quarantäne. Die Datei kann vom Quarantänemanager aus wiederhergestellt werden kann, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden. Je nach Datei stehen im Quarantänemanager noch weitere Auswahlmöglichkeiten zur Verfügung (siehe Quarantänemanager).

Löschen

Die Datei wird gelöscht. Dieser Vorgang ist bedeutend schneller als **Überschreiben und löschen** (siehe unten).

Ignorieren

Der Zugriff auf die Datei wird erlaubt und die Datei wird belassen.

Überschreiben und löschen

Der Echtzeit-Scanner überschreibt die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Warnung
Ist der Echtzeit-Scanner auf **Beim Schreiben durchsuchen** eingestellt, wird die betroffene Datei nicht erstellt.

Standard

Mit Hilfe dieser Schaltfläche können Sie die Aktion auswählen, die beim Fund eines Virus im Dialogfenster standardmäßig aktiviert ist. Markieren Sie die Aktion, die standardmäßig aktiviert sein soll, und klicken Sie auf die Schaltfläche "**Standard**".

Hinweis
Die Aktion **Reparieren** kann nicht als Standard-Aktion ausgewählt werden.

Weitere Informationen finden Sie hier.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der Echtzeit-Scanner reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Datei vor Aktion in Quarantäne kopieren

Bei aktivierter Option erstellt der Echtzeit-Scanner eine Sicherheitskopie (Backup) vor der Durchführung der gewünschten Primären bzw. Sekundären Aktion. Die Sicherheitskopie wird in der Quarantäne aufbewahrt. Sie kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat. Zudem können Sie die Sicherheitskopie an das Avira Malware Research Center

senden. Je nach Objekt stehen im Quarantänemanager noch weitere Auswahlmöglichkeiten zur Verfügung (siehe Quarantänemanager)

Primäre Aktion

Die primäre Aktion, ist die Aktion die ausgeführt wird, wenn der Echtzeit Scanner einen Virus bzw. ein unerwünschtes Programm findet. Ist die Option "**Reparieren**" gewählt, jedoch eine Reparatur der betroffenen Datei nicht möglich, wird die unter "**Sekundäre Aktion**" gewählte Aktion ausgeführt.

Hinweis
Die Option **Sekundäre Aktion** ist nur dann auswählbar, wenn unter **Primäre Aktion** die Einstellung **Reparieren** ausgewählt wurde.

Reparieren

Bei aktivierter Option repariert der Echtzeit Scanner betroffene Dateien automatisch. Wenn der Echtzeit-Scanner eine betroffene Datei nicht reparieren kann, führt es alternativ die unter **Sekundäre Aktion** gewählte Option aus.

Hinweis
Eine automatische Reparatur wird empfohlen, bedeutet aber, dass der Echtzeit Scanner Dateien auf dem Computer verändert.

Umbenennen

Bei aktivierter Option benennt der Echtzeit Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

Quarantäne

Bei aktivierter Option verschiebt der Echtzeit Scanner die Datei in ein Quarantäneverzeichnis. Die Dateien in diesem Verzeichnis können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

Ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.

Warnung
Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!



Überschreiben und löschen

Bei aktivierter Option überschreibt der Echtzeit Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Zugriff verweigern

Bei aktivierter Option trägt der Echtzeit Scanner den Fund nur in der Reportdatei ein, wenn die Reportfunktion aktiviert ist. Außerdem schreibt der Echtzeit Scanner einen Eintrag in das Ereignisprotokoll, wenn diese Option aktiviert ist.

> **Warnung**
> Ist der Echtzeit-Scanner auf **Beim Schreiben durchsuchen** eingestellt, wird die betroffene Datei nicht erstellt.

Sekundäre Aktion

Die Option "**Sekundäre Aktion"** ist nur dann auswählbar, wenn unter "**Primäre Aktion"** die Option "**Reparieren**" ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was mit der betroffenen Datei geschehen soll, wenn diese nicht reparabel ist.

Umbenennen

Bei aktivierter Option benennt der Echtzeit Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

Quarantäne

Bei aktivierter Option verschiebt der Echtzeit Scanner die Datei in Quarantäne. Die Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

Ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.

> **Warnung**
> Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Überschreiben und löschen

Bei aktivierter Option überschreibt der Echtzeit Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Zugriff verweigern

Bei aktivierter Option, wird die betroffene Datei nicht erstellt. Der Echtzeit-Scanner trägt den Fund nur in der Reportdatei ein, wenn die Reportfunktion aktiviert ist. Außerdem schreibt der Echtzeit-Scanner einen Eintrag in das Ereignisprotokoll, wenn diese Option aktiviert ist.

> **Hinweis**
> Wenn Sie als primäre oder sekundäre Aktion **Löschen** oder **Überschreiben und löschen** ausgewählt haben, beachten Sie bitte folgendes: Bei heuristischen Treffern werden die betroffenen Dateien nicht gelöscht, sondern in die Quarantäne verschoben.

Weitere Aktionen

Ereignisprotokoll verwenden

Bei aktivierter Option wird bei jedem Fund ein Eintrag in das Windows Ereignisprotokoll geschrieben. Die Ereignisse können in der Windows Ereignisanzeige abgerufen werden. Diese Einstellung ist standardmäßig aktiviert. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Ausnahmen

Mit diesen Optionen können Sie Ausnahme-Objekte für den Echtzeit-Scanner (Echtzeitsuche) konfigurieren. Die entsprechenden Objekte werden dann bei der Echtzeitsuche nicht beachtet. Der Echtzeit-Scanner kann über die Liste der auszulassenden Prozesse deren Dateizugriffe bei der Echtzeitsuche ignorieren. Dies ist zum Beispiel bei Datenbanken oder Backuplösungen sinnvoll. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Beachten Sie bei der Angabe von auszulassenden Prozessen und Dateiobjekten folgendes: Die Liste wird von oben nach unten abgearbeitet. Je länger die Liste ist, desto mehr Prozessorzeit braucht die Abarbeitung der Liste für jeden Zugriff. Halten Sie deshalb die Listen möglichst klein.

Vom Echtzeit-Scanner auszulassende Prozesse

Alle Dateizugriffe von Prozessen in dieser Liste werden von der Überwachung durch den Echtzeit-Scanner ausgenommen.

Eingabefeld

In dieses Feld geben Sie den Namen des Prozesses ein, der von der Echtzeitsuche nicht berücksichtigt werden soll. Standardmäßig ist kein Prozess eingegeben.

Der angegebene Pfad und der Dateiname des Prozesses dürfen maximal 255 Zeichen enthalten. Sie können bis zu 128 Prozesse eingeben. Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

Bei der Angabe des Prozesses werden Unicode-Zeichen akzeptiert. Sie können daher Prozess- oder Verzeichnisnamen angeben, die Sonderzeichen enthalten.

Laufwerke müssen wie folgt angegeben werden: `[Laufwerksbuchstabe]:\`

Das Zeichen Doppelpunkt (:) darf nur zur Angabe von Laufwerken verwendet werden.

Bei der Angabe des Prozesses können Sie die Platzhalter * (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) verwenden:

```
C:\Programme\Anwendung\anwendung.exe
C:\Programme\Anwendung\anwendun?.exe
C:\Programme\Anwendung\anwend*.exe
C:\Programme\Anwendung\*.exe
```

Um zu vermeiden, dass Prozesse global von der Überwachung des Echtzeit Scanners ausgenommen werden, sind Angaben ungültig, die ausschließlich aus folgenden Zeichen bestehen: * (Stern), ? (Fragezeichen), / (Slash), \ (Backslash), . (Punkt), : (Doppelpunkt).

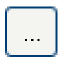
Sie haben die Möglichkeit, Prozesse ohne vollständige Pfadangabe von der Überwachung des Echtzeit-Scanners auszunehmen: `anwendung.exe`

Dies gilt jedoch ausschließlich für Prozesse, deren ausführbare Dateien auf Laufwerken der Festplatte liegen.

Eine vollständige Pfadangabe ist bei Prozessen erforderlich, deren ausführbare Dateien auf verbundenen Laufwerken, z.B. Netzlaufwerken liegen. Beachten Sie hierzu die allgemeinen Hinweise zur Notation von Ausnahmen auf verbundenen Netzlaufwerken.

Geben Sie keine Ausnahmen für Prozesse an, deren ausführbare Dateien auf dynamischen Laufwerken liegen. Dynamische Laufwerke werden für Wechseldatenträger wie CD, DVD oder USB-Stick verwendet.

Warnung
Bitte beachten Sie, dass alle Dateizugriffe, die von Prozessen initiiert werden und die in der Liste vermerkt wurden, von der Suche nach Viren und unerwünschten Programmen ausgeschlossen sind!



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, eine ausführbare Datei auszuwählen.

Prozesse

Die Schaltfläche "**Prozesse"** öffnet das Fenster "*Prozessauswahl*", in dem die laufenden Prozesse angezeigt werden.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen Prozess in das Anzeigefenster übernehmen.

Löschen

Mit der Schaltfläche entfernen Sie einen markierten Prozess aus dem Anzeigefenster.

Vom Echtzeit-Scanner auszulassende Dateiobjekte

Alle Dateizugriffe auf Objekte in dieser Liste werden von der Überwachung durch den Echtzeit-Scanner ausgenommen.

Eingabefeld

In dieses Feld geben Sie den Namen des Dateiobjekts ein, welches von der Echtzeitsuche nicht berücksichtigt wird. Standardmäßig ist kein Dateiobjekt eingegeben.

Die Einträge der Liste dürfen zusammen nicht mehr als 6000 Zeichen ergeben.

Bei der Angabe von auszulassenden Dateiobjekten können Sie die Platzhalter * (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) verwenden. Es können auch einzelne Dateierweiterungen ausgenommen werden (inklusive Platzhalter):

```
C:\Verzeichnis\*.mdb
*.mdb
*.md?
*.xls*
C:\Verzeichnis\*.log
```

Verzeichnisnamen müssen mit einem Backslash \ abgeschlossen sein.

Wenn ein Verzeichnis ausgenommen wird, werden automatisch auch alle darunter liegende Verzeichnisse mit ausgenommen.

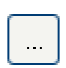
Pro Laufwerk können Sie maximal 20 Ausnahmen mit vollständigem Pfad (beginnend mit dem Laufwerksbuchstaben) angeben.

Bsp.: `C:\Programme\Anwendung\Name.log`

Die maximale Anzahl von Ausnahmen ohne vollständigen Pfad beträgt 64. Bsp:

```
*.log
 \Rechner1\C\Verzeichnis1
```

Bei dynamischen Laufwerken, die als Verzeichnis auf einem anderen Laufwerk eingebunden (gemountet) werden, müssen Sie den Aliasnamen des Betriebssystems für das eingebundene Laufwerk in der Liste der Ausnahmen verwenden:
z.B. `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
Verwenden Sie den Bereitstellungspunkt (mount point) selbst, z.B. `C:\DynDrive`, wird das dynamische Laufwerk trotzdem durchsucht. Sie können den zu verwendenden Aliasnamen des Betriebssystems aus der Report-Datei des Echtzeit-Scanners ermitteln.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, das gewünschte auszulassende Dateiobjekt auszuwählen.



Hinzufügen

Mit der Schaltfläche können Sie das im Eingabefeld eingegebene Dateiobjekt in das Anzeigefenster übernehmen.

Löschen

Mit der Schaltfläche Löschen entfernen Sie ein markiertes Dateiobjekt aus dem Anzeigefenster.

Beachten Sie bei der Angabe von Ausnahmen die weiteren Hinweise

Um Objekte auch dann auszunehmen, wenn darauf mit kurzen DOS-Dateinamen (DOS-Namenskonvention 8.3) zugegriffen wird, muss der entsprechende kurze Dateiname ebenfalls in die Liste eingetragen werden.

Ein Dateiname, der Platzhalter enthält, darf nicht mit einem Backslash abgeschlossen werden.
Beispielsweise:
`C:\Programme\Anwendung\anwend*.exe\`
Dieser Eintrag ist nicht gültig und wird nicht als Ausnahme behandelt!

Beachten Sie bei **Ausnahmen auf verbundenen Netzlaufwerken** folgendes: Wenn Sie den Laufwerksbuchstaben des verbundenen Netzlaufwerks verwenden, werden die angegebenen Dateien und Verzeichnisse NICHT von der Suche des Echtzeit-Scanners ausgenommen. Wenn der UNC-Pfad in der Liste der Ausnahmen vom UNC-Pfad, der zur Verbindung mit dem Netzlaufwerk genutzt wird, abweicht (Angabe von IP-Adresse in Liste der Ausnahmen - Angabe vom Computername zur Verbindung mit Netzlaufwerk) werden die angegebenen Verzeichnisse und Dateien NICHT von der Suche des Echtzeit-Scanners ausgenommen. Ermitteln Sie den zu verwendenden UNC-Pfad anhand der Report-Datei des Echtzeit-Scanners:
`\\<Computername>\<Freigabe>\` - ODER- `\\<IP-Adresse>\<Freigabe>\`

Anhand der Report-Datei des Echtzeit-Scanners können Sie die Pfade ermitteln, die der Echtzeit-Scanner bei der Suche nach betroffenen Dateien verwendet. Verwenden Sie grundsätzlich in der Liste der Ausnahmen dieselben Pfade. Gehen Sie wie folgt vor: Setzen Sie die Protokoll-Funktion des Echtzeit Scanners in der Konfiguration unter Report auf **Vollständig**. Greifen Sie nun mit dem aktivierten Echtzeit-Scanner auf die Dateien, Verzeichnisse, eingebundenen Laufwerke oder verbundenen Netzlaufwerke zu. Sie können nun den zu verwendenden Pfad aus der Reportdatei des Echtzeit-Scanners auslesen. Die Reportdatei rufen Sie im Control Center unter Echtzeit-Scanner ab.

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine. (Option nur bei aktiviertem Expertenmodus verfügbar.)

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den

Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD aktivieren

Ihr Avira Programm beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

10.3.2 Report

Der Echtzeit-Scanner besitzt eine umfangreiche Protokollierfunktion, die dem Benutzer bzw. dem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Echtzeit-Scanner kein Protokoll.
Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

Bei aktivierter Option nimmt der Echtzeit-Scanner wichtige Informationen (zu Fund, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt der Echtzeit-Scanner auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt der Echtzeit-Scanner sämtliche Informationen - auch solche zu Dateigröße, Dateityp, Datum etc. - in die Reportdatei auf.

Reportdatei beschränken

Größe beschränken auf n MB

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken. Erlaubte Werte zwischen 1 und 100 MB. Bei der Beschränkung der Reportdatei wird ein Spielraum von etwa 50 Kilobytes eingeräumt, um die Belastung des Rechners niedrig zu halten. Übersteigt die Größe der Protokolldatei die angegebene Größe um 50 Kilobytes, werden automatisch so lange alte Einträge gelöscht, bis die angegebene Größe weniger 50 Kilobytes erreicht worden ist.

Reportdatei vor dem Kürzen sichern

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert.

Konfiguration in Reportdatei schreiben

Bei aktivierter Option wird die verwendete Konfiguration der Echtzeitsuche in die Reportdatei geschrieben.

Hinweis
Wenn Sie keine Beschränkung der Reportdatei angegeben haben, wird automatisch eine neue Reportdatei angelegt, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es wird eine Sicherung der alten Reportdatei angelegt. Es werden bis zu drei Sicherungen alter Reportdateien vorgehalten. Die jeweils ältesten Sicherungen werden gelöscht.



10.4 Update

Unter der Rubrik **Update** konfigurieren Sie die automatische Ausführung von Updates. Sie haben die Möglichkeit, verschiedene Update-Intervalle einzustellen.

Automatisches Update

Alle n Tag(e) / Stunde(n) / Minute(n)

In diesem Feld können Sie das Intervall angeben, in dem automatische Updates ausgeführt werden sollen. Um das Update-Intervall zu ändern, markieren Sie eine der Zeitangaben im Feld und ändern Sie diese über die Pfeiltasten rechts vom Eingabefeld.

Auftrag zusätzlich bei Internet Verbindung starten

Bei aktivierter Option wird der Update-Auftrag zusätzlich zum festgelegten Update-Intervall bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.

Auftrag nachholen, wenn die Zeit bereits abgelaufen ist

Bei aktivierter Option werden Update-Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.

10.4.1 Web Server

Webserver

Das Update kann direkt über einen Webserver im Internet durchgeführt werden. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Verbindung zum Webserver

Vorhandene Verbindung (Netzwerk) verwenden

Diese Einstellung wird angezeigt, wenn Ihre Verbindung über ein Netzwerk verwendet wird.

Die folgende Verbindung verwenden

Diese Einstellung wird angezeigt, wenn Sie Ihre Verbindung individuell definieren.

Der Updater erkennt automatisch, welche Verbindungsoptionen vorhanden sind. Nicht vorhandene Verbindungsoptionen sind grau hinterlegt und können nicht aktiviert werden. Eine DFÜ-Verbindung können Sie z.B. manuell über einen Telefonbucheintrag in Windows herstellen.

Benutzer

Geben Sie den Benutzernamen Ihres ausgewählten Kontos ein.

Kennwort

Geben Sie das Kennwort für dieses Konto ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

Hinweis
Wenden Sie sich an den Internetdienstanbieter, wenn Sie den Benutzernamen oder das Kennwort eines vorhandenen Internetkontos vergessen haben.

Hinweis
Die automatische Einwahl des Updaters über sogenannte Dial-Up Tools (z.B. SmartSurfer, Oleco, ...) steht momentan noch nicht zur Verfügung.

Eine für das Update geöffnete DFÜ-Verbindung wieder beenden

Bei aktivierter Option wird die für das Update geöffnete DFÜ-Verbindung automatisch wieder unterbrochen, sobald der Download erfolgreich durchgeführt wurde.

Hinweis
Die Option ist unter Vista und Windows 7 nicht verfügbar. Unter Vista und Windows 7 wird die DFÜ-Verbindung, die für das Update geöffnet wurde, immer beendet, sobald der Download durchgeführt wurde.

Proxy Einstellungen

Proxyserver

Keinen Proxyserver verwenden

Bei aktivierter Option erfolgt Ihre Verbindung zum Webserver nicht über einen Proxyserver.

Windows Systemeinstellungen verwenden

Bei aktivierter Option werden die aktuellen Windows Systemeinstellungen für die Verbindung zum Webserver über einen Proxyserver verwendet. Sie konfigurieren die Windows Systemeinstellungen zur Verwendung eines Proxyservers unter **Systemsteuerung > Internetoptionen > Verbindungen > LAN-Einstellungen**. Im Internet Explorer können Sie im Menü **Extras** ebenfalls auf die Internetoptionen zugreifen.

Warnung
Wenn Sie einen Proxyserver nutzen, der eine Authentifizierung erfordert, geben Sie die Daten unter der Option **Verbindung über diesen Proxy** vollständig an.



> Die Option **Windows Systemeinstellungen verwenden** kann nur für Proxyserver ohne Authentifizierung genutzt werden.

Verbindung über diesen Proxyserver

Bei aktivierter Option erfolgt Ihre Verbindung zum Webserver über einen Proxyserver, wobei die von Ihnen angegebenen Einstellungen verwendet werden.

Adresse

Geben Sie den Rechnernamen oder die IP-Adresse des Proxyservers ein, den Sie für die Verbindung mit dem Webserver verwenden möchten.

Port

Geben Sie die Port-Nummer des Proxyservers ein, den Sie für die Verbindung mit dem Webserver verwenden möchten.

Login Name

Geben Sie einen Benutzernamen für die Anmeldung am Proxyserver ein.

Login Kennwort

Geben Sie das entsprechende Kennwort für die Anmeldung am Proxyserver ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

Beispiele:

Adresse: `proxy.domain.de` Port: `8080`

Adresse: `192.168.1.100` Port: `3128`

10.5 FireWall

Avira Antivirus Suite ermöglicht Ihnen, die Windows Firewall (ab Windows 7) zu verwalten:

- Avira FireWall
- Windows-Firewall

10.5.1 Windows-Firewall

Die Rubrik **FireWall** unter **Konfiguration > Internet Sicherheit** ist für die Konfiguration der Windows-Firewall in Betriebssystemen ab Windows 7 zuständig.

Netzwerkprofile

Netzwerkprofile

Basierend auf Netzwerkprofilen blockiert Windows-Firewall den Zugriff unbefugter Programme und Apps auf Ihren Computer:

- Privates Netzwerk: für Heim- oder Büro-Netzwerke
- Öffentliches Netzwerk: für öffentliche Netzwerke
- Domänennetzwerk: für Netzwerke mit einem Domänencontroller

Sie können diese Profile von der Konfiguration Ihres Avira Produkts verwalten, unter **Internet Sicherheit > Windows-Firewall > Netzwerkprofile**.

Für weitere Informationen über diese Netzwerkprofile, besuchen Sie die offizielle Microsoft-Webseite.

> **Warnung**
> Windows-Firewall wendet die gleichen Regeln für alle Netzwerke an, die zum selben Profil gehören. Das heißt, wenn Sie ein Programm oder eine App zulassen, hat diese auch Zugang zu allen Netzwerken, die das gleiche Profil verwenden.

Privates Netzwerk

Einstellungen für das private Netzwerk

Die Einstellungen für das private Netzwerk verwalten den Zugriff, den andere Computer oder Geräte in Ihrem Heim- oder Büronetzwerk auf Ihren Computer haben. Diese Einstellungen ermöglichen standardmäßig, dass die Benutzer des privaten Netzwerks Ihren Computer sehen und auf ihn zugreifen können.

Aktivieren

Bei aktivierter Option wird die Windows-Firewall eingeschaltet und durch Avira gesteuert.

Alle eingehenden Verbindungen blockieren

Bei aktivierter Option werden alle unerwünschten Versuche sich mit ihrem Computer zu verbinden von Windows-Firewall abgeleht, einschließlich eingehende Verbindungen von zugelassenen Anwendungen.

Benachrichtigen wenn eine neue App blockiert wird

Bei aktivierter Option werden Sie jedes Mal benachrichtigt, wenn ein Program oder eine App blockiert wird.

Deaktivieren (nicht empfohlen)

Bei aktivierter Option wird die Windows-Firewall ausgeschaltet. Diese Option wird nicht empfohlen, weil Ihr Computer dadurch gefährdet ist.



Öffentliches Netzwerk

Einstellungen für das öffentliche Netzwerk

Die Einstellungen für das öffentliche Netzwerk verwalten den Zugriff, den andere Computer oder Geräte in öffentlichen Netzwerken auf Ihren Computer haben. Diese Einstellungen ermöglichen standardmäßig nicht, dass die Benutzer des öffentlichen Netzwerks Ihren Computer sehen und auf ihn zugreifen können.

Aktivieren

Bei aktivierter Option wird die Windows-Firewall eingeschaltet und durch Avira gesteuert.

Alle eingehenden Verbindungen blockieren

Bei aktivierter Option werden alle unerwünschten Versuche sich mit ihrem Computer zu verbinden von Windows-Firewall abgeleht, einschließlich eingehende Verbindungen von zugelassenen Anwendungen.

Benachrichtigen wenn eine neue App blockiert wird

Bei aktivierter Option werden Sie jedes Mal benachrichtigt, wenn ein Program oder eine App blockiert wird.

Deaktivieren (nicht empfohlen)

Bei aktivierter Option wird die Windows-Firewall ausgeschaltet. Diese Option wird nicht empfohlen, weil Ihr Computer dadurch gefährdet ist.

Domänennetzwerk

Einstellungen für das Domänenetzwerk

Die Einstellungen für das Domänennetzwerk verwalten den Zugriff, den andere Computer oder Geräte auf Ihren Computer haben, wenn Ihr Computer mit einem über einen Domänencontroller authentifizierten Netzwerk verbunden ist. Diese Einstellungen ermöglichen standardmäßig, dass die authentifizierten Benutzer der Domäne Ihren Computer sehen und auf ihn zugreifen können.

Aktivieren

Bei aktivierter Option wird die Windows-Firewall eingeschaltet und durch Avira gesteuert.

Alle eingehenden Verbindungen blockieren

Bei aktivierter Option werden alle unerwünschten Versuche sich mit ihrem Computer zu verbinden von Windows-Firewall abgeleht, einschließlich eingehende Verbindungen von zugelassenen Anwendungen.

Benachrichtigen wenn eine neue App blockiert wird

Bei aktivierter Option werden Sie jedes Mal benachrichtigt, wenn ein Program oder eine App blockiert wird.

Deaktivieren (nicht empfohlen)

Bei aktivierter Option wird die Windows-Firewall ausgeschaltet. Diese Option wird nicht empfohlen, weil Ihr Computer dadurch gefährdet ist.

> **Hinweis**
> Diese Option ist nur verfügbar, wenn Ihr Computer mit einem Netzwerk verbunden ist, das über einen Domänencontroller verfügt.

Anwendungsregeln

Wenn Sie den Link unter **Windows-Firewall > Anwendungsregeln** klicken, werden Sie zum Menü **Zugelassene Apps und Features** der Windows-Firewall-Konfiguration weitergeleitet.

Erweiterte Einstellungen

Wenn Sie den Link unter **Windows-Firewall > Erweiterte Einstellungen** klicken, werden Sie zum Menü **Windows-Firewall mit erweiterter Sicherheit** der Windows-Firewall-Konfiguration weitergeleitet.

10.6 Browser-Schutz

Die Rubrik **Browser-Schutz** unter **Konfiguration > Internet Sicherheit** ist für die Konfiguration des Browser-Schutzes zuständig.

10.6.1 Suche

Mit dem Browser-Schutz schützen Sie sich vor Viren und Malware, die über Webseiten auf Ihren Computer gelangen, die Sie aus dem Internet in Ihren Webbrowser laden. In der Rubrik **Suche** können Sie das Verhalten des Browser-Schutzes einstellen. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Suche

IPv6 Unterstützung

Bei aktivierter Option wird die Internet-Protokoll-Version 6 vom Browser-Schutz unterstützt.

Drive-By Schutz



Unter *Drive-By Schutz* haben Sie die Möglichkeit, Einstellungen zum Blockieren von I-Frames, auch Inlineframes genannt, vorzunehmen. I-Frames sind HTML-Elemente, d.h. Elemente von Internetseiten, die einen Bereich einer Webseite abgrenzen. Mit I-Frames können andere Webinhalte - meist anderer URLs - als selbständige Dokumente in einem Unterfenster des Browsers geladen und angezeigt werden. Meist werden I-Frames für Banner-Werbung genutzt. In einigen Fällen werden I-Frames zum Verstecken von Malware verwendet. In diesen Fällen ist der Bereich des I-Frame im Browser meist kaum oder nicht sichtbar. Mit der Option **Verdächtige I-Frames blockieren** haben Sie die Möglichkeit, das Laden von I-Frames zu kontrollieren und zu blockieren.

Verdächtige I-Frames blockieren

Bei aktivierter Option werden I-Frames auf angeforderten Webseiten nach bestimmten Kriterien geprüft. Sind auf einer angeforderten Webseite verdächtige I-Frames vorhanden, wird das I-Frame blockiert. Im Fenster des I-Frames wird eine Fehlermeldung angezeigt.

Aktion bei Fund

Sie können Aktionen festlegen, die der Browser-Schutz ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Interaktiv

Bei aktivierter Option erscheint während der Direktsuche bei einem Fund eines Virus bzw. unerwünschten Programms ein Dialogfenster, in dem Sie auswählen können, was mit der betroffenen Datei weiter geschehen soll. Diese Einstellung ist standardmäßig aktiviert.

Fortschrittsbalken anzeigen

Bei aktivierter Option erscheint eine Desktopbenachrichtigung mit einem Download-Fortschrittsbalken, wenn ein Download oder das Herunterladen von Webseiten-Inhalten ein Timeout von 20 Sek. überschreitet. Diese Desktopbenachrichtigung dient insbesondere zur Kontrolle beim Herunterladen von Webseiten mit größerem Datenvolumen: Beim Surfen mit Browser-Schutz werden die Webseiteninhalte im Internet-Browser nicht sukzessive geladen, da sie vor der Anzeige im Internet-Browser nach Viren und Marlware durchsucht werden. Diese Option ist standardmäßig deaktiviert.

Weitere Informationen finden Sie hier.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der Browser-Schutz reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Primäre Aktion

Die primäre Aktion ist die Aktion, die ausgeführt wird, wenn der Browser-Schutz einen Virus bzw. ein unerwünschtes Programm findet.

Zugriff verweigern

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt. Der Browser-Schutz trägt den Fund in die Reportdatei ein, vorausgesetzt die Reportfunktion ist aktiviert.

In Quarantäne verschieben

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden beim Fund eines Virus bzw. einer Malware in die Quarantäne verschoben. Die betroffene Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Ignorieren

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom Browser-Schutz an Ihren Webbrowser weitergeleitet. Der Zugriff auf die Datei wird erlaubt und die Datei wird belassen.

> **Warnung**
> Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Gesperrte Zugriffe

Unter **Gesperrte Zugriffe** können Sie Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) angeben, die vom Browser-Schutz blockiert werden sollen. Mit dem Web-Filter können Sie bekannte, unerwünschte URLs, wie z.B. Phishing- und Malware-URLs, blockieren. Der Browser-Schutz verhindert die Übertragung der Daten vom Internet auf Ihr Computersystem. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Vom Browser-Schutz zu blockierende Dateitypen / MIME-Typen

Alle Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) in der Liste werden vom Browser-Schutz blockiert.

Eingabefeld

In diesem Feld geben Sie die Namen der MIME-Typen und Dateitypen ein, die vom Browser-Schutz blockiert werden sollen. Für Dateitypen geben Sie die Datei-Extension ein, z.B. **.htm**. Für MIME-Typen notieren Sie den Medientyp und ggf. den Subtyp. Beide Angaben werden durch einen einfachen Schrägstrich voneinander getrennt, z.B. **video/mpeg** oder **audio/x-wav**.

> **Hinweis**
> Dateien, die bereits auf Ihrem Computersystem als temporäre Internetdateien gespeichert worden sind, werden zwar vom Browser-Schutz blockiert, können jedoch vom Internet-Browser lokal von Ihrem Computer geladen werden. Temporäre Internetdateien sind Dateien, die vom Internet-Browser auf Ihrem Computer gesichert werden, um Webseiten schneller anzeigen zu können.

> **Hinweis**
> Die Liste der zu blockierenden Datei- und MIME-Typen wird bei Einträgen in der Liste der auszulassenden Datei- und MIME-Typen unter Ausnahmen ignoriert.

> **Hinweis**
> Bei der Angabe von Dateitypen und MIME-Typen können Sie keine Wildcards (Platzhalter * für beliebig viele Zeichen oder ? für genau ein Zeichen) verwenden.

MIME-Typen: Beispiele für Medientypen

- `text` = für Textdateien
- `image` = für Grafikdateien
- `video` = für Videodateien
- `audio` = für Sound-Dateien
- `application` = für Dateien, die an ein bestimmtes Programm gebunden sind

Beispiele: Auszulassende Datei- und MIME-Typen

- `application/octet-stream` = Dateien des MIME-Typs application/octet-stream (ausführbare Dateien *.bin, *.exe, *.com, *dll, *.class) werden vom Browser-Schutz blockiert.
- `application/olescript` = Dateien des MIME-Typs application/olescript (ActiveX Skript-Dateien *.axs) werden vom Browser-Schutz blockiert.
- `.exe` = Alle Dateien mit der Dateierweiterung .exe (ausführbare Dateien) werden vom Browser-Schutz blockiert.
- `.msi` = Alle Dateien mit der Dateierweiterung .msi (Windows Installer Dateien) werden vom Browser-Schutz blockiert.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen MIME- oder Dateityp in das Anzeigefenster übernehmen.



Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Web-Filter

Der Web-Filter verfügt über eine interne und täglich aktualisierte Datenbank, in der URLs nach Inhaltskriterien klassifiziert sind.

Web-Filter aktivieren

Bei aktivierter Option werden alle URLs, die zu den ausgewählten Kategorien in der Web-Filter-Liste zählen, blockiert.

Web-Filter-Liste

In der Web-Filter-Liste können Sie die Inhaltskategorien wählen, deren URLs vom Browser-Schutz blockiert werden sollen.

> **Hinweis**
> Der Web-Filter wird bei Einträgen in der Liste der auszulassenden URLs unter Ausnahmen ignoriert.

> **Hinweis**
> Unter **Spam URLs** werden URLs kategorisiert, die mit Spam-Emails verbreitet werden. Die Kategorie **Betrug / Täuschung** umfasst Webseiten mit 'Abonnement-Fallen' und anderen Angeboten von Dienstleistungen, deren Kosten vom Anbieter verschleiert werden.

Ausnahmen

Mit diesen Optionen können Sie MIME-Typen (Inhaltstypen der übertragenen Daten) und Dateitypen für URLs (Internetadressen) von der Suche des Browser-Schutzes ausschließen. Die angegebenen MIME-Typen und URLs werden vom Browser-Schutz ignoriert, d.h. diese Daten werden beim Übertragen auf Ihr Computersystem nicht auf Viren und Malware durchsucht.

Vom Browser-Schutz auszulassende MIME-Typen

In diesem Feld können Sie die MIME-Typen (Inhaltstypen der übertragenen Daten) auswählen, die von der Suche des Browser-Schutzes ausgenommen werden sollen.

Vom Browser-Schutz auszulassende Dateitypen / MIME-Typen (benutzerdefiniert)

Alle Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) in der Liste werden von der Suche des Browser-Schutzes ausgenommen.

Eingabefeld

In diesem Feld geben Sie die Namen der MIME-Typen und Dateitypen ein, die von der Suche des Browser-Schutzes ausgenommen werden sollen. Für Dateitypen geben Sie die Datei-Extension ein, z.B. **.htm**. Für MIME-Typen notieren Sie den Medientyp und ggf. den Subtyp. Beide Angaben werden durch einen einfachen Schrägstrich voneinander getrennt, z.B. **video/mpeg** oder **audio/x-wav**.

Hinweis
Bei der Angabe von Dateitypen und MIME-Typen können Sie keine Wildcards (Platzhalter * für beliebig viele Zeichen oder ? für genau ein Zeichen) verwenden.

Warnung
Alle Dateitypen und Inhaltstypen auf der Ausschlussliste werden ohne weitere Prüfung der gesperrten Zugriffe (Liste der zu blockierenden Datei- und MIME-Typen unter Browser-Schutz > Suche > Gesperrte Zugriffe) oder des Browser-Schutzes im Internet-Browser geladen: Bei allen Einträgen auf der Ausschlussliste werden die Einträge der Liste der zu blockierenden Datei- und MIME-Typen ignoriert. Es wird keine Suche nach Viren und Malware ausgeführt.

MIME-Typen: Beispiele für Medientypen:

- `text` für Textdateien
- `image` = für Grafikdateien
- `video` = für Videodateien
- `audio` = für Sound-Dateien
- `application` = für Dateien, die an ein bestimmtes Programm gebunden sind

Beispiele: Auszulassende Datei-und MIME-Typen:

- `audio/` = Alle Dateien vom Medientyp Audio werden von der Suche des Browser-Schutzes ausgenommen
- `video/quicktime` = Alle Videodateien vom Subtyp Quicktime (*.qt, *.mov) werden von der Suche des Browser-Schutzes ausgenommen
- `.pdf` = Alle Adobe-PDF-Dateien sind von der Suche des Browser-Schutzes ausgenommen.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen MIME- oder Dateityp in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Vom Browser-Schutz auszulassende URLs

Alle URLs in dieser Liste werden von der Suche des Browser-Schutzes ausgenommen.

Eingabefeld

In diesem Feld geben Sie URLs (Internetadressen) an, die von der Suche des Browser-Schutzes ausgenommen werden sollen, z.B. `www.domainname.com`. Sie können Teile der URL angeben, wobei Sie mit abschließenden oder führenden Punkten den Domain-Level kennzeichnen: `.domainname.de` für alle Seiten und alle Subdomains der Domain. Eine Webseite mit beliebiger Top-Level-Domain (`.com` oder `.net`) notieren Sie mit einem abschließendem Punkt: `domainname.`. Wenn Sie eine Zeichenfolge ohne führenden oder abschließenden Punkt notieren, wird die Zeichenfolge als Top-Level-Domain interpretiert, z.B. `net` für alle NET-Domains (`www.domain.net`).

Hinweis
Bei der Angabe von URLs können Sie auch das Wildcard-Zeichen * für beliebig viele Zeichen verwenden. Verwenden Sie auch in Kombination mit Wildcards abschließende oder führende Punkte, um die Domain-Levels zu kennzeichnen:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (gültig aber nicht empfohlen)
Angaben ohne Punkte wie *`name`* werden als Teile einer Top-Level-Domain interpretiert und sind nicht sinnvoll.

Warnung
Alle Webseiten auf der Liste der auszulassenden URLs werden ohne weitere Prüfung des Web-Filters oder des Browser-Schutzes im Internet-Browser geladen: Bei allen Einträgen in der Liste der auszulassenden URLs werden Einträge des Web-Filters (siehe Browser-Schutz > Suche > Gesperrte Zugriffe) ignoriert. Es wird keine Suche nach Viren und Malware ausgeführt. Schließen Sie deshalb nur vertrauenswürdige URLs von der Suche des Browser-Schutzes aus.

Hinzufügen

Mit der Schaltfläche können Sie die im Eingabefeld eingegebene URL (Internetadresse) in das Anzeigefenster übernehmen.



Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Beispiele: Auszulassende URLs

- `www.avira.com` -ODER- `www.avira.com/*`
  = Alle URLs mit der Domain `www.avira.com` werden von der Suche des Browser-Schutzes ausgenommen: *.avira.com/en/pages/index.php*, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*, usw. URLs mit der Domain `www.avira.de` sind nicht von der Suche des Browser-Schutzes ausgenommen.
- `avira.com` -ODER- `*.avira.com`
  = Alle URLs mit der Second- und Top-Level-Domain `avira.com` werden von der Suche des Browser-Schutzes ausgenommen. Die Angabe impliziert alle existierenden Subdomains zu `.avira.com`: *www.avira.com*, *forum.avira.com*, usw.
- `avira.` -ODER- `*.avira.*`
  = Alle URLs mit der Second-Level-Domain `avira` werden von der Suche des Browser-Schutzes ausgenommen. Die Angabe impliziert alle existierenden Top-Level-Domains oder Subdomains zu `.avira.`: *www.avira.com*, *www.avira.de*, *forum.avira.com*, usw.
- `.*domain*.*`
  = Alle URLs, die eine Second-Level-Domain mit der Zeichenkette `domain` enthalten, werden von der Suche des Browser-Schutzes ausgenommen: *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...
- `net` -ODER- `*.net`
  = Alle URLs mit der Top-Level-Domain `net` werden von der Suche des Browser-Schutzes ausgenommen: *www.name1.net*, *www.name2.net*, usw.

> **Warnung**
> Geben Sie die URLs, die Sie von der Suche des Browser-Schutzes ausschließen möchten, so präzise wie möglich an. Vermeiden Sie die Angabe gesamter Top-Level-Domains oder Teile eines Second-Level-Domainnamens, da die Gefahr besteht, dass Internetseiten, die Malware und unerwünschte Programme verbreiten durch globale Angaben unter Ausnahmen von der Suche des Browser-Schutzes ausgeschlossen werden. Es wird empfohlen mindestens die vollständige Second-Level-Domain und die Top-Level-Domain anzugeben: `domainname.com`

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den

Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD aktivieren

Ihr Avira Produkt beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware, mit Fehlmeldungen muss jedoch gerechnet werden.

10.6.2 Report

Der Browser-Schutz besitzt eine umfangreiche Protokollierfunktion, die dem Benutzer bzw. dem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Browser-Schutz kein Protokoll.
Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

Bei aktivierter Option nimmt der Browser-Schutz wichtige Informationen (zu Funden, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt der Browser-Schutz auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt der Browser-Schutz sämtliche Informationen - auch solche zu Dateigröße, Dateityp, Datum etc. - in die Reportdatei auf.

Reportdatei beschränken

Größe beschränken auf n MB

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken; mögliche Werte: 1 bis 100 MB. Bei der Beschränkung der Reportdatei wird ein Spielraum von etwa 50 Kilobytes eingeräumt, um die Belastung des Rechners niedrig zu halten. Übersteigt die Größe der Protokolldatei die angegebene Größe um 50 Kilobytes, werden automatisch so lange alte Einträge gelöscht, bis die angegebene Größe weniger 20% erreicht worden ist.

Konfiguration in Reportdatei schreiben

Bei aktivierter Option wird die verwendete Konfiguration der Echtzeitsuche in die Reportdatei geschrieben.

> **Hinweis**
> Wenn Sie keine Beschränkung der Reportdatei angegeben haben, werden automatisch ältere Einträge gelöscht, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es werden so viele Einträge gelöscht bis die Reportdatei eine Größe von 80 MB erreicht hat.

10.7 Email-Schutz

Die Rubrik Email-Schutz der Konfiguration ist für die Konfiguration des Email-Schutzes zuständig.

10.7.1 Suche

Sie nutzen den Email-Schutz, um eingehende Emails auf Viren und Malware zu prüfen. Ausgehende Emails können vom Email-Schutz auf Viren und Malware geprüft werden.

Eingehende Emails durchsuchen

Bei aktivierter Option werden eingehende Emails auf Viren und Malware geprüft. Email Schutz unterstützt die Protokolle POP3 und IMAP. Aktivieren Sie das Posteingangs-Konto, welches von Ihrem Email-Client zum Empfang von Emails genutzt wird, zur Überwachung durch den Email-Schutz.

POP3-Konten überwachen

Bei aktivierter Option werden die POP3-Konten an den angegebenen Ports überwacht.

Überwachte Ports

In diesem Feld geben Sie den Port ein, der als Posteingang vom Protokoll POP3 genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von POP3 zurück.

IMAP-Konten überwachen

Bei aktivierter Option werden die IMAP-Konten an den angegebenen Ports überwacht.

Überwachte Ports

In diesem Feld geben Sie den Port ein, der vom Protokoll IMAP genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von IMAP zurück.

Ausgehende Emails durchsuchen (SMTP)

Bei aktivierter Option werden ausgehende Emails auf Viren und Malware geprüft.

Überwachte Ports

In diesem Feld geben Sie den Port ein, der als Postausgang vom Protokoll SMTP genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von SMTP zurück.



> **Hinweis**
> Um die genutzten Protokolle und Ports zu verifizieren, rufen Sie in Ihrem Email-Client-Programm die Eigenschaften Ihrer Email-Konten ab. Meist werden Standard-Ports genutzt.

IPv6 Unterstützung

Bei aktivierter Option wird die Internet-Protokoll-Version 6 von Email-Schutz unterstützt. (Option nicht für Neu- oder Änderungsinstallationen unter Windows 8 verfügbar.)

Aktion bei Fund

Diese Konfigurationsrubrik enthält Einstellungen, welche Aktionen durchgeführt werden, wenn Email-Schutz einen Virus bzw. unerwünschtes Programm in einer Email oder in einem Anhang findet. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

> **Hinweis**
> Die hier eingestellten Aktionen erfolgen sowohl bei einem Virenfund in eingehenden Emails als auch bei einem Virenfund in ausgehenden Emails.

Interaktiv

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms in einer Email oder einem Anhang ein Dialogfenster, in dem Sie auswählen können, was mit der betroffenen Email bzw. dem Anhang geschehen soll. Diese Option ist standardmäßig aktiviert.

Fortschrittsbalken anzeigen

Bei aktivierter Option blendet der Email-Schutz während des Downloads von Emails eine Fortschrittsanzeige ein. Eine Aktivierung dieser Option ist nur möglich, wenn die Option **Interaktiv** ausgewählt wurde.

Automatisch

Bei aktivierter Option werden Sie bei Fund eines Virus bzw. unerwünschten Programms nicht mehr benachrichtigt. Der Email-Schutz reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Betroffene Emails

Die unter "*Betroffene Emails*" gewählte Option wird als primäre Aktion ausgeführt , wenn der Email-Schutz einen Virus bzw. ein unerwünschtes Programm in einer Email findet. Ist die Option "**Ignorieren"** gewählt, kann unter "*Betroffene Anhänge*" zusätzlich ausgewählt werden, was im Falle eines Funds in einem Anhang geschehen soll.



Löschen

Bei aktivierter Option wird die betroffene Email beim Fund eines Virus bzw. unerwünschten Programms automatisch gelöscht. Der Textkörper der Email (Body) wird hierbei durch den unten angegebenen Standardtext ersetzt. Gleiches gilt für alle enthaltenen Anlagen (Attachments); diese werden ebenfalls durch einen Standardtext ersetzt.

Ignorieren

Bei aktivierter Option wird die betroffene Email trotz des Funds eines Virus bzw. unerwünschten Programms ignoriert. Sie haben jedoch noch die Möglichkeit zu entscheiden, was mit einem betroffenen Anhang geschehen soll.

In Quarantäne verschieben

Bei aktivierter Option wird die komplette Email inkl. aller Anhänge beim Fund eines Virus bzw. unerwünschten Programms in Quarantäne gestellt. Sie kann später - falls gewünscht - wieder hergestellt werden. Die betroffene Email selbst wird gelöscht. Der Textkörper der Email (Body) wird hierbei durch den unten angegebenen Standardtext ersetzt. Gleiches gilt für alle enthaltenen Anlagen (Attachments); diese werden ebenfalls durch einen Standardtext ersetzt.

Betroffene Anhänge

Die Option "**Betroffene Anhänge**" ist nur dann auswählbar, wenn unter "*Betroffene Emails*" die Einstellung "**Ignorieren**" ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was im Fall eines Funds in einem Anhang geschehen soll.

Löschen

Bei aktivierter Option wird der betroffene Anhang beim Fund eines Virus bzw. unerwünschten Programms gelöscht und durch einen Standardtext ersetzt.

Ignorieren

Bei aktivierter Option wird der Anhang trotz des Funds eines Virus bzw. unerwünschten Programms ignoriert und zugestellt.

Warnung
Wenn Sie diese Option wählen, haben Sie keinerlei Schutz vor Viren und unerwünschten Programmen durch den Email-Schutz. Wählen Sie diesen Punkt nur dann, wenn Sie genau wissen, was Sie tun. Deaktivieren Sie die Vorschau in Ihrem Email-Programm, starten Sie Anhänge auf keinen Fall per Doppelklick!

In Quarantäne verschieben

Bei aktivierter Option wird der betroffene Anhang in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Der betroffene Anhang kann später - falls gewünscht - wieder hergestellt werden.



Andere Aktionen

Diese Konfigurationsrubrik enthält weitere Einstellungen, welche Aktionen durchgeführt werden, wenn der Email-Schutz einen Virus bzw. unerwünschtes Programm in einer Email oder in einer Anlage findet. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

> **Hinweis**
> Die hier eingestellten Aktionen erfolgen ausschließlich bei einem Virenfund in eingehenden Emails.

Standardtext für gelöschte und verschobene Emails

Der Text in diesem Feld wird anstelle der betroffenen Email als Nachricht in die Email eingefügt. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombination kann zum Formatieren verwendet werden:

Strg + Enter = Fügt einen Zeilenumbruch ein.

Standard

Die Schaltfläche fügt einen vordefinierten Standardtext in das Editierfeld ein.

Standardtext für gelöschte und verschobene Anlagen

Der Text in diesem Feld wird anstelle der betroffenen Anlage als Nachricht in die Email eingefügt. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombination kann zum Formatieren verwendet werden:

Strg + Enter = Fügt einen Zeilenumbruch ein.

Standard

Die Schaltfläche fügt einen vordefinierten Standardtext in das Editierfeld ein.

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine. (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu

geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD aktivieren

Ihr Avira Produkt beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

10.7.2 Allgemeines

Ausnahmen

Email-Adressen, die nicht überprüft werden

Diese Tabelle zeigt Ihnen die Liste der Email-Adressen, die von der Überprüfung durch den Avira Email-Schutz ausgeschlossen wurden (Whitelist).

> **Hinweis**
> Die Liste der Ausnahmen wird ausschließlich bei eingehenden Emails vom Email-Schutz verwendet.

Email-Adressen, die nicht überprüft werden

Eingabefeld

In diesem Feld geben Sie die Email-Adresse ein, die Sie in die Liste der nicht zu prüfenden Email-Adressen hinzufügen wollen. Die Email-Adresse wird in Zukunft - abhängig von Ihren Einstellungen - nicht mehr vom Email Schutz überprüft.

Hinzufügen

Mit der Schaltfläche können Sie die im Eingabefeld eingegebene Email-Adresse der Liste der nicht zu prüfenden Email-Adressen hinzufügen.

Löschen

Die Schaltfläche löscht eine markierte Email-Adresse in der Liste.

Email-Adresse

Email-Adresse, die nicht mehr durchsucht werden soll.

Malware

Bei aktivierter Option wird die Email-Adresse nicht mehr auf Malware überprüft.

nach oben

Mit dieser Schaltfläche verschieben Sie eine markierte Email-Adresse um eine Position nach oben. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist oder die markierte Adresse auf der ersten Position in der Liste steht.

nach unten

Mit dieser Schaltfläche verschieben Sie eine markierte Email-Adresse um eine Position nach unten. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist oder die markierte Adresse auf der letzten Position in der Liste steht.

Zwischenspeicher

Der Email-Schutz Zwischenspeicher enthält die Daten zu den durchsuchten Emails, die in der Statistik im Control Center unter **Email-Schutz** angezeigt werden.

Maximale Anzahl von Emails im Zwischenspeicher

In diesem Feld wird die maximale Anzahl der Emails eingegeben, die der Email-Schutz im Zwischenspeicher aufbewahrt. Es werden jeweils die ältesten Emails gelöscht.

Maximale Speicherung einer Email in Tagen

In diesem Feld ist die maximale Speicherdauer einer Email in Tagen eingegeben. Nach dieser Zeit wird die Email aus dem Zwischenspeicher entfernt.

Zwischenspeicher leeren

Bei Klick auf die Schaltfläche werden die Emails, die im Zwischenspeicher aufbewahrt werden, gelöscht.

10.7.3 Report

Der Email-Schutz besitzt eine umfangreiche Protokollierfunktion, die dem Benutzer bzw. dem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Email-Schutz kein Protokoll.
Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

Bei aktivierter Option nimmt der Email-Schutz wichtige Informationen (zu Fund, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt der Email-Schutz auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt der Email-Schutz sämtliche Informationen in die Reportdatei auf.

Reportdatei beschränken

Größe beschränken auf n MB

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken; mögliche Werte: 1 bis 100 MB. Bei der Beschränkung der Reportdatei wird ein Spielraum von etwa 50 Kilobytes eingeräumt, um die Belastung des Rechners niedrig zu halten. Übersteigt die Größe der Protokolldatei die angegebene Größe um 50 Kilobytes, werden automatisch so lange alte Einträge gelöscht, bis die angegebene Größe weniger 50 Kilobytes erreicht worden ist.

Reportdatei vor dem Kürzen sichern

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert.

Konfiguration in Reportdatei schreiben

Bei aktivierter Option wird die verwendete Konfiguration des Email-Schutzes in die Reportdatei geschrieben.

> **Hinweis**
> Wenn Sie keine Beschränkung der Reportdatei angegeben haben, wird automatisch eine neue Reportdatei angelegt, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es wird eine Sicherung der alten Reportdatei angelegt. Es werden bis zu drei Sicherungen alter Reportdateien vorgehalten. Die jeweils ältesten Sicherungen werden gelöscht.

10.8 Allgemeines

10.8.1 Gefahrenkategorien

Auswahl erweiterter Gefahrenkategorien (Optionen nur bei aktiviertem Expertenmodus verfügbar)

Ihr Avira Produkt schützt Sie vor Computerviren. Darüber hinaus haben Sie die Möglichkeit, differenziert nach folgenden Gefahrenkategorien suchen zu lassen.

- Adware
- Adware/Spyware
- Anwendungen
- Backdoor-Steuersoftware
- Dateien mit verschleierten Dateiendungen
- Kostenverursachende Einwahlprogramme
- Phishing
- Programme, die die Privatsphäre verletzen
- Scherzprogramme
- Spiele
- Trügerische Software
- Ungewöhnliche Laufzeitpacker

Durch einen Klick auf das entsprechende Kästchen wird der gewählte Typ aktiviert (Häkchen gesetzt) bzw. deaktiviert (kein Häkchen).

Alle aktivieren

Bei aktivierter Option werden sämtliche Typen aktiviert.



Standardwerte

Diese Schaltfläche stellt die vordefinierten Standardwerte wieder her.

> **Hinweis**
> Wird ein Typ deaktiviert, werden Dateien, die als entsprechender Programmtyp erkannt werden, nicht mehr gemeldet. Es erfolgt auch kein Eintrag in die Reportdatei.

10.8.2 Erweiterter Schutz

Erweiterter Schutz

ProActiv (Option nur bei aktiviertem Expertenmodus verfügbar.)

ProActiv aktivieren

Bei aktivierter Option werden Programme auf Ihrem Computersystem überwacht und auf verdächtige Aktionen überprüft. Tritt ein Verhalten auf, das für Malware typisch ist, erhalten Sie eine Meldung. Sie können das Programm blockieren oder mit "**Ignorieren**" die Ausführung des Programms fortsetzen. Von der Überwachung ausgenommen sind: Als vertrauenswürdig eingestufte Programme, vertrauenswürdige und signierte Programme, die standardmäßig im Anwendungsfilter der erlaubten Anwendungen enthalten sind, alle Programme, die Sie zum Anwendungsfilter der erlaubten Programme hinzugefügt haben.

Mit dem Einsatz von ProActiv schützen Sie sich vor neuen und unbekannten Bedrohungen, für die noch keine Virendefinitionen und Heuristiken vorliegen. Die ProActiv-Technologie ist in die Komponente Echtzeit-Scanner integriert und beobachtet und analysiert die ausgeführten Aktionen von Programmen. Das Verhalten von Programmen wird auf typische Aktionsmuster von Malware untersucht: Art der Aktion und Aktionsabfolgen. Falls ein Programm ein für Malware typisches Verhalten zeigt, wird dies wie ein Virenfund behandelt und gemeldet : Sie haben die Möglichkeit, die Ausführung des Programms zu blockieren oder die Meldung zu ignorieren und die Ausführung des Programms fortzusetzen. Sie können das Programm als vertrauenswürdig einstufen und so zum Anwendungsfilter der erlaubten Programme hinzufügen. Sie haben auch die Möglichkeit, das Programm über die Anweisung **Immer blockieren** zum Anwendungsfilter der zu blockierenden Programme hinzuzufügen.

Zur Ermittlung des verdächtigen Verhaltens verwendet die ProActiv-Komponente Regelsets, die vom Avira Malware Research Center entwickelt wurden. Die Regelsets werden von den Avira Datenbanken gespeist. Zur Informationserfassung in den Avira Datenbanken sendet ProActiv Informationen über gemeldete, verdächtige Programme. Während der Installation von Avira, haben Sie die Möglichkeit, die Datenübermittlung an die Avira Datenbanken zu deaktivieren.

> **Hinweis**
> Die ProActiv-Technologie ist für 64-Bit-Systeme noch nicht verfügbar!

Cloud-Sicherheit (Optionen nur bei aktiviertem Expertenmodus verfügbar.)

Cloud-Sicherheit aktivieren

Fingerabdrücke aller verdächtigen Dateien werden zur dynamischen Online-Erkennung an Avira Cloud übertragen. Anwendungsdateien werden sofort als sauber, infiziert oder unbekannt angezeigt.

Das Cloud-Sicherheitssystem fungiert als zentraler Knotenpunkt, um Cyber-Attacken auf die Avira-Community zu erkennen. Die Dateien, auf die Ihr PC zugreift, werden mit den Mustern der Dateien abgeglichen, die im Cloud-System gespeichert sind. Da die Hauptarbeit in der Cloud stattfindet, benötigt das lokale Schutzprogramm weniger Ressourcen.

Es wird eine Liste von Dateispeicherorten erstellt, auf welche Malware-Programme abzielen, bei jeder **Schnelle Systemprüfung**. In dieser Liste sind zum Beispiel laufende Prozesse, Start- und Dienstprogramme enthalten. Von jeder Datei wird eine digitale Prüfsumme ("Fingerabdruck") erstellt, an das Cloud-Sicherheitssystem gesendet und dann als "Clean" oder "Malware" entsprechend eingestuft. Unbekannte Programmdateien werden zur Analyse in das Cloud-Sicherheitssystem hochgeladen.

Manuell bestätigen, wenn verdächtige Dateien an Avira gesendet werden

Sie können die Liste der verdächtigen Dateien, die zur Cloud-Sicherheit hochgeladen werden sollen, prüfen und selber auswählen, welche Dateien Sie hochladen möchten.

Zu blockierende Anwendungen

Unter *Zu blockierende Anwendungen* können Sie Anwendungen einpflegen, die Sie als schädlich einstufen und die von Avira ProActiv standardmäßig geblockt werden sollen. Die eingepflegten Anwendungen können auf Ihrem Computersystem nicht ausgeführt werden. Sie können Programme dem Anwendungsfilter für zu blockierende Anwendungen auch über die Meldungen des Echtzeit-Scanners zu einem verdächtigen Programmverhalten hinzufügen, indem Sie die Option **Dieses Programm immer blockieren** nutzen.

Zu blockierende Anwendungen

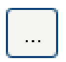
Anwendung

In der Liste sind alle Anwendungen aufgeführt, die Sie als schädlich eingestuft und über die Konfiguration oder über die Meldungen der ProActiv-Komponente eingefügt haben. Die Anwendungen der Liste werden von Avira ProActiv blockiert und können auf Ihrem Computersystem nicht ausgeführt werden. Beim Start eines zu blockierenden Programms erscheint eine Meldung des Betriebssystems. Die zu blockierenden Anwendungen werden von Avira ProActiv anhand des angegebenen Pfads und des Dateinamens identifiziert und unabhängig von ihrem Inhalt blockiert.



Eingabefeld

In diesem Feld geben Sie die Anwendung an, die blockiert werden soll. Zur Identifizierung der Anwendung müssen der vollständige Pfad und der Dateiname mit Dateiendung angegebenen werden. Die Pfadangabe muss entweder das Laufwerk, auf dem die Anwendung liegt, enthalten oder mit einer Umgebungsvariablen beginnen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die zu blockierende Anwendung auszuwählen.

Hinzufügen

Mit der Schaltfläche "**Hinzufügen"** können Sie die im Eingabefeld angegebene Anwendung in die Liste der zu blockierenden Anwendungen übernehmen.

> **Hinweis**
> Anwendungen, die für die Funktionsfähigkeit des Betriebssystems erforderlich sind, können nicht hinzugefügt werden.

Löschen

Mit der Schaltfläche "**Löschen"** entfernen Sie eine markierte Anwendung aus der Liste der zu blockierenden Anwendungen.

Auszulassende Anwendungen

Unter *Auszulassende Anwendungen* sind Anwendungen gelistet, die von der Überwachung der ProActiv-Komponente ausgenommen sind: Signierte Programme, die als vertrauenswürdig eingestuft wurden und standardmäßig in der Liste enthalten sind, alle Anwendungen, die Sie als vertrauenswürdig eingestuft und in den Anwendungsfilter eingepflegt haben: Sie können in der Konfiguration Anwendungen zur Liste der erlaubten Anwendungen hinzufügen. Sie haben auch die Möglichkeit, über die Meldungen des Echtzeit-Scanners zu einem verdächtigen Programmverhalten Anwendungen hinzuzufügen, indem Sie in der Echtzeit-Scanner-Meldung die Option **Vertrauenswürdiges Programm** nutzen.

Auszulassende Anwendungen

Anwendung

Die Liste enthält Anwendungen, die von der Überwachung der ProActiv Komponente ausgenommen sind. In den Standardeinstellungen nach der Installation enthält die Liste signierte Anwendungen von vertrauenswürdigen Herstellern. Sie haben die Möglichkeit, Anwendungen, die Sie als vertrauenswürdig einstufen, über die Konfiguration oder über Meldungen des Echtzeit-Scanners einzupflegen. Die ProActiv-Komponente identifiziert Anwendungen anhand des Pfades, des Dateinamens und des Inhalts. Eine Inhaltsprüfung ist sinnvoll, da einem Programm über Veränderungen wie Updates nachträglich Schadcode hinzugefügt werden kann. Sie können über den

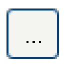
angegebenen **Typ** festlegen, ob eine Inhaltsprüfung erfolgen soll: Beim Typ "*Inhalt*" werden die mit Pfad und Dateinamen angegebenen Anwendungen auf Veränderungen des Dateiinhalts geprüft, bevor Sie von der Überwachung durch die ProActiv-Komponente ausgenommen werden. Bei einem veränderten Dateiinhalt wird die Anwendung von der ProActiv-Komponente wieder überwacht. Beim Typ "*Pfad*" erfolgt keine Inhaltsüberprüfung, bevor die Anwendung von der Überwachung durch den Echtzeit-Scanner ausgenommen wird. Um den Ausschlusstyp zu wechseln, klicken Sie den angezeigten Typ an.

Warnung
Verwenden Sie den Typ *Pfad* nur in Ausnahmefällen. Durch ein Update kann einer Anwendung Schadcode hinzugefügt werden. Die ursprünglich harmlose Anwendung ist nun Malware.

Hinweis
Einige vertrauenswürdige Anwendungen, wie z.B. alle Anwendungskomponenten Ihres Avira Produktes, sind standardmäßig von einer Überwachung durch die ProActiv-Komponente ausgenommen, sind aber in der Liste nicht aufgeführt.

Eingabefeld

In diesem Feld geben Sie die Anwendung an, die von der Überwachung durch die ProActiv-Komponente ausgenommen werden soll. Zur Identifizierung der Anwendung müssen der vollständige Pfad und der Dateiname mit Dateiendung angegebenen werden. Die Pfadangabe muss entweder das Laufwerk, auf dem die Anwendung liegt, enthalten oder mit einer Umgebungsvariablen beginnen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die auszulassende Anwendung auszuwählen.

Hinzufügen

Mit der Schaltfläche "**Hinzufügen"** können Sie die im Eingabefeld angegebene Anwendung in die Liste der auszulassenden Anwendungen übernehmen.

Löschen

Mit der Schaltfläche "**Löschen"** entfernen Sie eine markierte Anwendung aus der Liste der auszulassenden Anwendungen.

10.8.3 Passwort

Sie können Ihr Avira Produkt in unterschiedlichen Bereichen durch ein Kennwort schützen. Wurde ein Kennwort vergeben, werden Sie jedes Mal nach diesem Kennwort gefragt, wenn Sie den jeweils geschützten Bereich öffnen wollen.

Passwort

Kennwort eingeben

Geben Sie hier Ihr gewünschtes Kennwort ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt. Sie können maximal 20 Zeichen eingeben. Ist das Kennwort einmal angegeben, verweigert das Programm bei Angabe eines falschen Kennworts den Zugriff. Ein leeres Feld bedeutet "Kein Kennwort".

Bestätigung

Geben Sie hier das oben eingetragene Kennwort zur Bestätigung erneut ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

> **Hinweis**
> Groß- und Kleinschreibung wird unterschieden!

Kennwort geschützte Bereiche

Ihr Avira Produkt kann einzelne Bereiche durch ein Kennwort schützen. Durch Klick auf das entsprechende Kästchen kann die Kennwortabfrage für einzelne Bereiche nach Wunsch deaktiviert bzw. wieder aktiviert werden.

Kennwortgeschützer Bereich	Funktion
Control Center	Bei aktivierter Option wird zum Start des Control Center das gesetzte Kennwort benötigt.
Echtzeit-Scanner aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung von Avira Echtzeit-Scanner das gesetzte Kennwort benötigt.
Email-Schutz aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung des Email-Schutzes das gesetzte Kennwort benötigt.
Browser-Schutz aktivieren/ deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung des Browser-Schutzes das gesetzte Kennwort benötigt.

Quarantäne	Bei aktivierter Option wird zum Aktivieren bzw. Deaktivieren allen Bereichen des Quarantänemanagers das gesetzte Kennwort benötigt. Durch Klick auf das entsprechende Kästchen, kann die Kennwortabfrage nach Wunsch deaktiviert bzw. wieder aktiviert werden.
Wiederherstellen betroffener Objekte	Bei aktivierter Option wird zum Wiederherstellen eines Objekts das gesetzte Kennwort benötigt.
Erneutes Prüfen betroffener Objekte	Bei aktivierter Option wird zum erneuten Prüfen eines Objekts das gesetzte Kennwort benötigt.
Eigenschaften betroffener Objekte	Bei aktivierter Option wird zur Anzeige der Eigenschaften eines Objekts das gesetzte Kennwort benötigt.
Löschen betroffener Objekte	Bei aktivierter Option wird für das Löschen eines Objekts das gesetzte Kennwort benötigt.
Email an Avira senden	Bei aktivierter Option wird für das Versenden eines Objekts zur Überprüfung an das Avira Malware Research Center das gesetzte Kennwort benötigt.
Konfiguration	Bei aktivierter Option ist die Konfiguration des Programms nur nach Eingabe des gesetzten Kennworts möglich.
Installation / Deinstallation	Bei aktivierter Option wird zur Installation bzw. Deinstallation des Programms das gesetzte Passwort benötigt.

10.8.4 Sicherheit

Optionen nur bei aktiviertem Expertenmodus verfügbar.

Autorun

Autorun-Funktion blockieren

Bei aktivierter Option wird die Ausführung der Windows Autorun-Funktion auf allen eingebundenen Laufwerken wie USB-Sticks, CD- und DVD-Laufwerken, Netzlaufwerken blockiert. Mit der Windows Autorun-Funktion werden Dateien auf Datenträgern oder Netzlaufwerken beim Einlegen oder beim Verbinden sofort gelesen, Dateien können so automatisch gestartet und wiedergegeben werden. Diese Funktionalität birgt jedoch ein hohes Sicherheitsrisiko, da mit dem automatischen Start von Dateien Malware und unerwünschte Programme installiert werden können. Besonders kritisch ist die Autorun-Funktion für USB-Sticks, da sich Daten auf einem Stick ständig ändern können.

CDs und DVDs ausnehmen

Bei aktivierter Option wird die Autorun-Funktion auf CD- und DVD-Laufwerken zugelassen.

> **Warnung**
> Deaktivieren Sie die Autorun-Funktion für CD- und DVD-Laufwerke nur dann, wenn Sie sicher sind, dass Sie ausschließlich vertrauenswürdige Datenträger verwenden.

Systemschutz

Windows hosts Datei vor Änderungen schützen

Ist diese Option aktiviert, ist die Windows hosts Datei schreibgeschützt. Eine Manipulation der Datei ist dann nicht länger möglich. Malware ist dann beispielsweise nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten. Diese Option ist standardmäßig aktiviert.

Produktschutz

> **Hinweis**
> Die Optionen zum Produktschutz sind nicht verfügbar, wenn der Echtzeit Scanner bei einer benutzerdefinierten Installation nicht installiert wurde.

Prozesse vor unerwünschtem Beenden schützen

Bei aktivierter Option werden alle Prozesse des Programms vor unerwünschtem Beenden durch Viren und Malware oder vor einem 'unkontrollierten' Beenden durch einen Benutzer z.B. via Task-Manager geschützt. Diese Option ist standardmäßig aktiviert.

Erweiterter Prozessschutz

Bei aktivierter Option werden alle Prozesse des Programms vor unerwünschtem Beenden mit erweiterten Methoden geschützt. Der erweiterte Prozessschutz benötigt erheblich mehr Rechnerressourcen als der einfache Prozessschutz. Die Option ist



standardmäßig aktiviert. Zum Deaktivieren der Option ist ein Rechnerneustart erforderlich.

Hinweis
Der Prozessschutz ist unter Windows XP 64 Bit nicht verfügbar!

Warnung
Bei aktiviertem Prozessschutz können Interaktionsprobleme mit anderen Softwareprodukten auftreten. Deaktivieren Sie in diesen Fällen den Prozessschutz.

Dateien und Registrierungseinträge vor Manipulation schützen

Bei aktivierter Option werden alle Registry-Einträge des Programms sowie alle Dateien des Programms (Binär- und Konfigurationsdateien) vor Manipulation geschützt. Der Schutz vor Manipulation beinhaltet den Schutz vor schreibendem, löschendem und z.T. lesendem Zugriff auf die Registry-Einträge oder die Programmdateien durch Benutzer oder fremde Programme. Zum Aktivieren der Option ist ein Rechnerneustart erforderlich.

Warnung
Beachten Sie, dass bei deaktivierter Option die Reparatur von Computern, die mit bestimmten Arten von Malware infiziert sind, fehlschlagen kann.

Hinweis
Bei aktivierter Option sind Änderungen an der Konfiguration, so auch die Änderung von Prüf- oder Update-Aufträgen nur über die Benutzeroberfläche möglich.

Hinweis
Der Schutz von Dateien und Registrierungseinträgen ist unter Windows XP 64 Bit nicht verfügbar!

10.8.5 WMI

Optionen nur bei aktiviertem Expertenmodus verfügbar.

Unterstützung für Windows Management Instrumentation (WMI)

Windows Management Instrumentation ist eine grundlegende Windows Verwaltungstechnologie, die es ermöglicht mittels Skript- und Programmiersprachen

lesend und schreibend, lokal und remote auf Einstellungen von Windows Rechnern zuzugreifen. Ihr Avira Produkt unterstützt WMI und stellt Daten (Statusinformationen, Statistik-Daten, Reports, geplante Aufträge etc.) sowie Ereignisse an einer Schnittstelle zur Verfügung. Sie haben über WMI die Möglichkeit, Betriebsdaten des Programms abzurufen.

WMI-Unterstützung aktivieren

Bei aktivierter Option haben Sie die Möglichkeit, über WMI Betriebsdaten des Programms abzurufen.

10.8.6 Ereignisse

Optionen nur bei aktiviertem Expertenmodus verfügbar.

Größe der Ereignisdatenbank begrenzen

Größe begrenzen auf maximal n Einträge

Bei aktivierter Option kann die maximale Anzahl der Einträge in der Ereignisdatenbank auf eine bestimmte Größe begrenzt werden; erlaubte Werte sind: 100 bis 10 000 Einträge. Wird die Anzahl der eingegebenen Einträge überschritten, werden die jeweils ältesten Einträge gelöscht.

Alle Ereignisse löschen älter als n Tag(e)

Bei aktivierter Option werden Ereignisse nach einer gewissen Anzahl von Tagen aus der Ereignisdatenbank gelöscht; erlaubte Werte sind: 1 bis 90 Tage. Diese Option ist standardmäßig mit einem Wert von 30 Tagen aktiviert.

Keine Begrenzung

Bei aktivierter Option ist die Größe der Ereignisdatenbank nicht begrenzt. Auf der Programmoberfläche unter Ereignisse werden jedoch maximal 20 000 Einträge angezeigt.

10.8.7 Berichte

Optionen nur bei aktiviertem Expertenmodus verfügbar.

Berichte begrenzen

Anzahl begrenzen auf maximal n Stück

Bei aktivierter Option kann die maximale Anzahl von Berichten auf eine bestimmte Menge begrenzt werden; erlaubte Werte sind: 1 bis 300. Wird die angegebene Anzahl überschritten, werden die jeweils ältesten Berichte gelöscht.

Alle Berichte löschen älter als n Tag(e)

Bei aktivierter Option werden Berichte nach einer gewissen Anzahl von Tagen automatisch gelöscht; erlaubte Werte sind: 1 bis 90 Tage. Diese Option ist standardmäßig mit einem Wert von 30 Tagen aktiviert.

Keine Begrenzung

Bei aktivierter Option ist die Anzahl der Berichte nicht begrenzt.

10.8.8 Verzeichnisse

Optionen nur bei aktiviertem Expertenmodus verfügbar.

Temporärer Pfad

Systemeinstellung verwenden

Bei aktivierter Option werden für die Handhabung von temporären Dateien die Einstellungen des Systems verwendet.

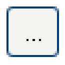
> **Hinweis**
> Wo Ihr System temporäre Dateien speichert finden Sie - am Beispiel von Windows XP - unter: **Start > Einstellungen > Systemsteuerung > System >** Registerkarte "**Erweitert**" > Schaltfläche "**Umgebungsvariablen**". Die temporären Variablen (`TEMP`, `TMP`) für den jeweils angemeldeten Benutzer als auch für Systemvariablen (`TEMP`, `TMP`) sind hier mit ihren entsprechenden Werten ersichtlich.

Folgendes Verzeichnis verwenden

Bei aktivierter Option wird der im Eingabefeld angezeigte Pfad verwendet.

Eingabefeld

In diesem Eingabefeld tragen Sie den Pfad ein, unter dem temporäre Dateien vom Programm abgelegt werden sollen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, den gewünschten temporären Pfad auszuwählen.

Standard

Die Schaltfläche stellt das vordefinierte Verzeichnis für den temporären Pfad wieder her.

10.8.9 Akustische Warnung

Optionen nur bei aktiviertem Expertenmodus verfügbar.



Beim Fund eines Virus oder einer Malware durch den System-Scanner oder den Echtzeit-Scanner ertönt im interaktiven Aktionsmodus ein Warnton. Sie haben die Möglichkeit, den Warnton zu deaktivieren oder zu aktivieren sowie eine alternative WAVE-Datei als Warnton auszuwählen.

> **Hinweis**
> Der Aktionsmodus des System-Scanners wird in der Konfiguration unter PC Sicherheit > System-Scanner > Suche > Aktion bei Fund eingestellt. Der Aktionsmodus des Echtzeit-Scanners wird in der Konfiguration unter PC Sicherheit > Echtzeit-Scanner > Suche > Aktion bei Fund eingestellt.

Keine Warnung

Bei aktivierter Option erfolgt keine akustische Warnung bei einem Virenfund durch den System-Scanner oder den Echtzeit-Scanner.

Über PC-Lautsprecher abspielen (nur bei interaktivem Modus)

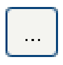
Bei aktivierter Option erfolgt eine akustische Warnung mit dem Standardwarnton beim Fund eines Virus durch den System-Scanner oder den Echtzeit-Scanner. Der Warnton wird über den PC internen Lautsprecher abgespielt.

Folgende WAVE-Datei benutzen (nur bei interaktivem Modus)

Bei aktivierter Option erfolgt bei Fund eines Virus durch den System-Scanner oder den Echtzeit-Scanner ein akustisches Warnen mit der ausgewählten WAVE-Datei. Die ausgewählte WAVE-Datei wird über einen angeschlossenen externen Lautsprecher abgespielt.

WAVE-Datei

In diesem Eingabefeld können Sie den Namen und den dazugehörigen Pfad einer Audiodatei Ihrer Wahl eintragen. Der Standardwarnton des Programms ist als Voreinstellung eingetragen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei mit Hilfe des Datei-Explorers auszuwählen.

Test

Diese Schaltfläche dient zum Testen der ausgewählten WAVE-Datei.

10.8.10 Warnungen

Ihr Avira Produkt erzeugt bei bestimmten Ereignissen Desktopbenachrichtigungen, sogenannte Slide-Ups, um Sie über Gefahren sowie erfolgreich ausgeführte oder fehlgeschlagene Programmabläufe, wie z.B. die Ausführung eines Updates, zu informieren. Unter **Warnungen** können Sie die Benachrichtigung bei bestimmten Ereignissen aktivieren oder deaktivieren.



Bei Desktop-Benachrichtigungen besteht die Möglichkeit, die Benachrichtigung direkt im Slide-Up zu deaktivieren. Sie können die Deaktivierung der Benachrichtigung im Konfigurationsfenster **Warnungen** rückgängig machen.

Update

Warnung, falls letztes Update älter als n Tag(e) ist

In diesem Feld können Sie die Anzahl an Tagen eingeben, die seit dem letzten Update maximal vergangen sein dürfen. Ist dieser Zeitraum überschritten, wird im Control Center unter Status ein rotes Icon für den Update-Status angezeigt.

Hinweis anzeigen, falls Virendefinitionsdatei veraltet

Bei aktivierter Option erhalten Sie im Fall einer veralteten Virendefinitionsdatei eine Warnmeldung. Mit Hilfe der Option "Warnung, falls letztes Update älter als n Tag(e)" können Sie den zeitlichen Abstand zur Warnmeldung konfigurieren.

Warnungen / Hinweise bei folgenden Situationen

Dial-Up Verbindung wird verwendet

Bei aktivierter Option werden Sie mit einer Desktop-Benachrichtigung gewarnt, wenn auf Ihrem Rechner ein Einwahlprogramm über das Telefon- oder das ISDN-Netz eine Wählverbindung aufbaut. Es besteht die Gefahr, dass es sich bei dem Einwahlprogramm um einen unbekannten und unerwünschten Dialer handelt, der eine kostenpflichtige Verbindung erstellt. (siehe Gefahrenkategorien: Kostenverursachende Einwahlprogramme)

Dateien wurden erfolgreich aktualisiert

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update erfolgreich abgeschlossen wurde und Dateien aktualisiert wurden.

Update ist fehlgeschlagen

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update fehlgeschlagen ist: Es konnte keine Verbindung zum Downloadserver aufgebaut werden oder die Update-Dateien konnten nicht installiert werden.

Es ist kein Update notwendig

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update angestoßen wurde, die Installation von Dateien jedoch nicht erforderlich war, da Ihr Programm auf dem aktuellsten Stand ist.

11. Tray Icon

Das Tray Icon im Systemtray der Taskleiste zeigt den Status des Echtzeit Scanners an.

Symbol	Beschreibung
	Avira Echtzeit-Scanner ist aktiviert
	Avira Echtzeit-Scanner ist deaktiviert

Einträge im Kontextmenü

- **Echtzeit Scanner aktivieren**: Aktiviert bzw. deaktiviert den Avira Echtzeit Scanner.
- **Email-Schutz aktivieren**: Aktiviert bzw. deaktiviert den Avira Email-Schutz.
- **Browser Schutz aktivieren**: Aktiviert bzw. deaktiviert den Avira Browser Schutz.
- **Avira Antivirus Suite starten**: Öffnet das Control Center.
- **Avira Antivirus Suite konfigurieren**: Öffnet die Konfiguration.
- **Meine Meldungen**: Öffnet ein Slide-Up mit aktuellsten Meldungen zu Ihrem Avira Produkt.
- **Meine Kommunikationseinstellungen**: Öffnet das Abo-Center für Produktmitteilungen
- **Update starten**: Startet ein Update.
- **Hilfe**: Öffnet die Online-Hilfe.
- **Experts Market**: öffnet die Webseite Experts Market - Hilfe anfordern. Dort können Sie um Hilfe bitten oder anderen Anwendern Ihre Hilfe anbieten.
- **Über Avira Antivirus Suite**:
  Öffnet ein Dialogfenster mit Informationen zu Ihrem Avira Produkt: Produktinformationen, Versionsinformationen, Lizenzinformationen.
- **Avira im Internet**:
  Öffnet das Avira Webportal im Internet. Voraussetzung ist, dass Sie einen aktiven Zugang zum Internet haben.

12. Produkt Benachrichtigungen

12.1.1 Abo-Center für Produktmitteilungen

Durch Klicken auf *Meine Kommunikations-Einstellungen* im Kontextmenü des Avira Tray Icon oder durch Klicken des Symbols für **Konfiguration** im Slide-Up **Meine Meldungen** erreichen Sie das **Abo-Center für Produktmitteilungen** auf unserer Webseite.

- Sie haben die Möglichkeit, den Informationsfluss der Produktmitteilungen zu steuern, indem Sie auf die entsprechenden **AN/AUS** Schaltflächen klicken.
- Klicken Sie anschließend auf **Profil aktualisieren**, um Ihr persönliches Benachrichtigungsprofil zu hinterlegen.
  - ↳ Sie erhalten die Meldung, dass Ihr Benachrichtigungsprofil erfolgreich aktualisiert wurde.

Treten Sie Online mit uns in Kontakt, indem Sie auf einen der Links klicken.

12.1.2 Aktuelle Meldungen

Das Slide-Up *Meine Meldungen* dient als Kommunikationsschnittstelle. Es informiert Sie über die neuesten Entwicklungen in der Internet Sicherheit, Neuigkeiten zu Avira Produkten (Updates, Upgrades und Lizenzbenachrichtigungen) und zeigt aktuelle Vireninformationen.

Liegen keine neuen Meldungen vor, erhalten Sie die Nachricht *Es sind keine neuen Meldungen vorhanden*. Klicken Sie **OK**, um das Slide-Up zu schließen.

Sie haben folgende Möglichkeiten, wenn neue Meldungen vorliegen:

- Klicken Sie **Später erinnern,** um die aktuellen Meldungen zu einem späteren Zeitpunkt zu lesen.
- Klicken Sie **+ mehr**, um die Details der Meldung zu lesen.
  - ↳ Abhängig von der Art der Meldung, werden Sie auf unsere Webseite weitergeleitet oder erhalten Informationen in einem neuen Fenster.
- Klicken Sie auf das kleine Kreuz **x**, um einzelne Meldungen zu schließen.
- Klicken Sie auf das Symbol für **Konfiguration** in der Kopfzeile des Slide-Up, um Ihr persönliches Benachrichtigungsprofil zu hinterlegen.

13. FireWall

Avira Antivirus Suite ermöglicht Ihnen den ein- und ausgehenden Datenverkehr anhand Ihrer Computereinstellungen zu überwachen und zu regeln:

- Windows-Firewall

Ab Windows 7 erlaubt Avira Antivirus Suite das Verwalten der Windows-Firewall durch das Avira Produkt.

13.1 Windows-Firewall

Sie haben die Möglichkeit, die Windows-Firewall mithilfe des Control- und Konfigurationscenters zu steuern. Dabei haben Sie folgende Möglichkeiten die Windows-Firewall einzustellen:

Windows-Firewall im Control Center aktivieren

Sie können die Windows-Firewall aktivieren oder deaktivieren, indem Sie die Schaltfläche **AN/AUS** der Option *FireWall* unter **Status > Internet Sicherheit** klicken.

Den Status der Windows-Firewall im Control Center überprüfen

Sie können den Status der Windows-Firewall unter der Rubrik **INTERNET SICHERHEIT > FireWall** überprüfen und die empfohlenen Einstellungen wiederherstellen, indem Sie die Schaltfläche **Problem beheben** klicken.

14. Updates

14.1 Updates

Die Wirksamkeit einer Antivirensoftware steht und fällt mit der Aktualität des Programms, insbesondere der Virendefinitionsdatei und der Suchengine. Zur Ausführung von Updates ist die Komponente Updater in Ihr Avira Produkt integriert. Der Updater sorgt dafür, dass Ihr Avira Produkt stets auf dem neuesten Niveau arbeitet und in der Lage ist, die täglich neu erscheinenden Viren zu erfassen. Der Updater aktualisiert die folgenden Komponenten:

- Virendefinitionsdatei:

  Die Virendefinitionsdatei enthält die Erkennungsmuster der Schadprogramme, die Ihr Avira Produkt bei der Suche nach Viren und Malware sowie bei der Reparatur von betroffenen Objekten verwendet.

- Suchengine:

  Die Suchengine enthält die Methoden, mit denen Ihr Avira Produkt nach Viren und Malware sucht.

- Programmdateien (Produktupdate):

  Updatepakete für Produktupdates stellen weitere Funktionen für die einzelnen Programmkomponenten zur Verfügung.

Bei der Ausführung eines Updates werden die Virendefinitionsdatei und die Suchengine auf Aktualität geprüft und bei Bedarf aktualisiert. Je nach den Einstellungen in der Konfiguration führt der Updater zusätzlich ein Produktupdate durch oder benachrichtigt Sie über verfügbare Produktupdates. Nach einem Produktupdate kann ein Neustart Ihres Computersystems erforderlich sein. Erfolgt nur ein Update der Virendefinitionsdatei und der Suchengine, muss der Rechner nicht neu gestartet werden.

> **Hinweis**
> Aus Sicherheitsgründen prüft der Updater, ob die Windows hosts-Datei Ihres Computers dahingehend geändert wurde, ob die Update-URL beispielsweise durch Malware manipuliert wurde und den Updater auf unerwünschte Download-Seiten umleitet. Wurde die Windows hosts-Datei manipuliert, so ist dies in der Updater Reportdatei ersichtlich.

Ein Update wird in folgendem Intervall automatisch ausgeführt: 2 Stunden.

Im Control Center unter **Planer** können Sie weitere Update-Aufträge einrichten, die in den angegebenen Intervallen vom Updater ausgeführt werden. Sie haben auch die Möglichkeit, ein Update manuell zu starten:

- Im Control Center: Im Menü **Update** und in der Rubrik **Status**

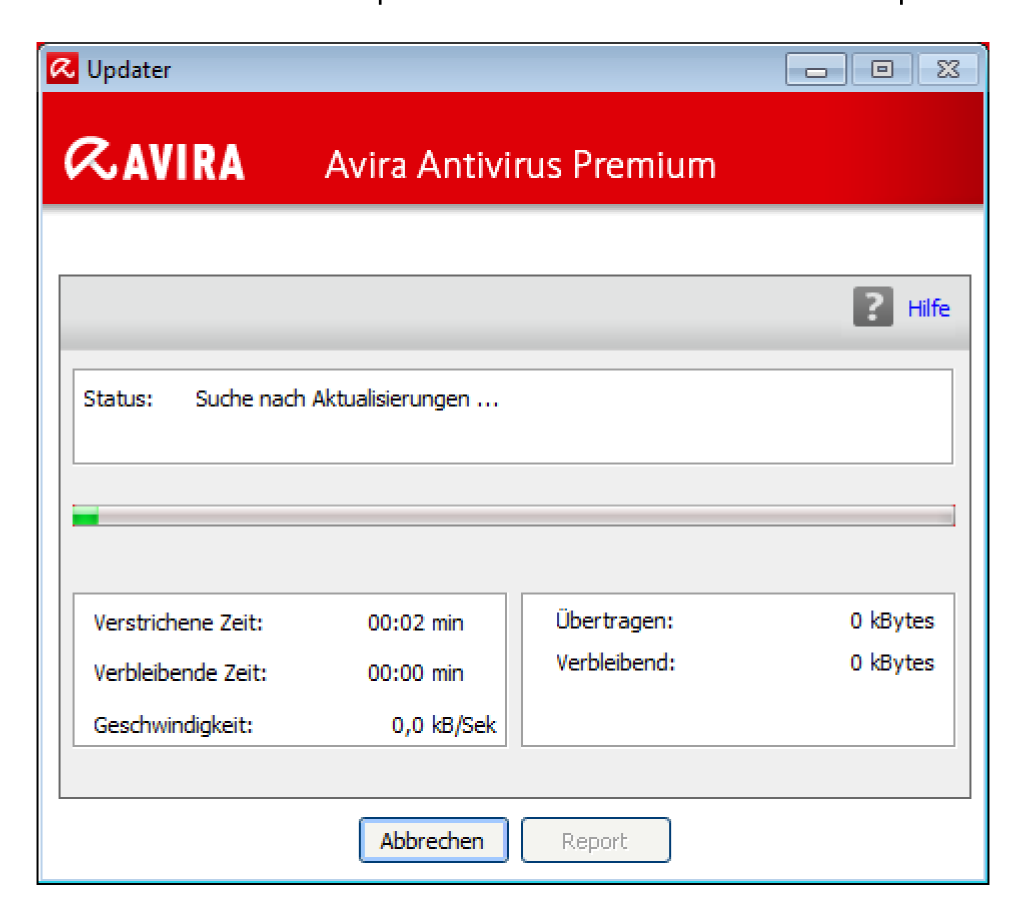


- Über das Kontextmenü des Tray Icons

Sie beziehen Updates aus dem Internet über einen Webserver des Herstellers. Standardmäßig wird die existierende Netzwerkverbindung als Verbindung zu den Avira Downloadservern genutzt. Sie können diese Standardeinstellung in der Konfiguration unter Allgemeines > Update anpassen.

14.2 Updater

Nach dem Start eines Updates öffnet sich das Fenster des Updaters.



Hinweis
Bei Update-Aufträgen, die Sie im Planer anlegen, können Sie den **Darstellungsmodus** für das Update-Fenster einstellen: Sie können zwischen den Darstellungsmodi **Unsichtbar**, **Minimiert** oder **Maximiert** wählen.

Hinweis
Arbeiten Sie mit einem Programm im Vollbildmodus (z.B. Spiele) und der Updater befindet sich im Darstellungsmodus maximiert oder minimiert, schaltet der Updater kurzzeitig auf den Desktop um. Um dies zu verhindern, können Sie

den Updater auch im Darstellungsmodus unsichtbar starten lassen. Sie werden so bei einem Update nicht mehr durch das Update-Fenster benachrichtigt.

Status: Zeigt das momentane Vorgehen des Updaters.

Aktuelle Datei: Name der Datei, die gerade heruntergeladen wird.

Verstrichene Zeit: Zeit, die seit dem Start des Downloadvorgangs vergangen ist.

Verbleibende Zeit: Zeit, bis der Downloadvorgang abgeschlossen ist.

Geschwindigkeit: Geschwindigkeit, mit der die Dateien heruntergeladen werden.

Heruntergeladene Bytes: Bereits heruntergeladene Bytes.

Restliche Bytes: Noch herunterzuladende Bytes.

Schaltflächen und Links

Schaltfläche / Link	Beschreibung
Hilfe	Über diese Schaltfläche bzw. den Link wird diese Seite der Online-Hilfe geöffnet.
Reduzieren	Das Anzeigefenster des Updaters wird verkleinert dargestellt.
Vergrößern	Das Anzeigefenster des Updaters wird auf die ursprüngliche Größe wieder hergestellt.
Abbrechen	Der Updatevorgang wird abgebrochen. Der Updater wird geschlossen.
Beenden	Der Updatevorgang ist abgeschlossen. Das Anzeigefenster wird geschlossen.
Report	Die Reportdatei des Updates wird angezeigt.

15. Problembehebung, Tipps

In diesem Kapitel finden Sie wichtige Hinweise zur Behebung von Problemen und weitere Tipps zum Umgang mit Ihrem Avira Produkt.

- siehe Kapitel Hilfe im Problemfall
- siehe Kapitel Tastaturbefehle
- siehe Kapitel Windows Sicherheitscenter (für Windows XP) oder Windows Wartungscenter (ab Windows 7)

15.1 Hilfe im Problemfall

Hier finden Sie Informationen zu Ursachen und Lösungen möglicher Probleme.

- Die Fehlermeldung *Die Lizenzdatei lässt sich nicht öffnen* erscheint.
- Die Fehlermeldung *Der Verbindungsaufbau schlug fehl beim Downloaden der Datei ...* erscheint beim Versuch, ein Update zu starten.
- Viren und Malware können nicht verschoben oder gelöscht werden.
- Das Tray Icon zeigt einen deaktivierten Zustand an.
- Der Rechner wird extrem langsam, wenn ich eine Datensicherung durchführe.
- Meine Firewall meldet den Avira Echtzeit-Scanner und Avira Email-Schutz sobald diese aktiv sind.
- Avira Email-Schutz funktioniert nicht.
- Eine Email, die über eine TLS-Verbindung versendet wurde, wurde vom Email-Schutz blockiert.
- Webchat funktioniert nicht: Chat-Nachrichten werden nicht angezeigt; im Browser werden Daten geladen

Die Fehlermeldung *Die Lizenzdatei lässt sich nicht öffnen* erscheint.

Ursache: Die Datei ist verschlüsselt.

- Zur Aktivierung der Lizenz müssen Sie die Datei nicht öffnen, sondern im Programmverzeichnis speichern.

Die Fehlermeldung *Der Verbindungsaufbau schlug fehl beim Downloaden der Datei ...* erscheint beim Versuch, ein Update zu starten.

Ursache: Ihre Internetverbindung ist inaktiv. Deshalb kann keine Verbindung zum Webserver im Internet erstellt werden.

- Testen Sie, ob andere Internetdienste wie WWW oder Email funktionieren. Wenn nicht, stellen Sie die Internetverbindung wieder her.

Ursache: Der Proxyserver ist nicht erreichbar.

- Prüfen Sie, ob sich das Login für den Proxyserver geändert hat und passen Sie gegebenenfalls Ihre Konfiguration an.

Ursache: Die Datei *update.exe* ist bei Ihrer Firewall nicht vollständig freigegeben.

- Stellen Sie sicher, dass die Datei *update.exe* bei Ihrer Firewall vollständig freigegeben ist.

Ansonsten:

- Prüfen Sie in der Konfiguration unter PC Sicherheit > Update.

Viren und Malware können nicht verschoben oder gelöscht werden.

Ursache: Die Datei wurde von Windows geladen und befindet sich in einem aktiven Zustand.

- Aktualisieren Sie Ihr Avira Produkt.
- Wenn Sie das Betriebssystem Windows XP verwenden, deaktivieren Sie die Systemwiederherstellung.
- Starten Sie den Computer im abgesicherten Modus.
- Öffnen Sie die Konfiguration Ihres Avira Produkts .
- Wählen Sie **System-Scanner > Suche > Dateien > Alle Dateien** und bestätigen Sie das Fenster mit **OK**.
- Starten Sie einen Suchlauf über alle lokalen Laufwerke.
- Starten Sie den Computer im normalen Modus.
- Führen Sie einen Suchlauf im normalen Modus durch.
- Falls keine weiteren Viren und Malware gefunden werden, aktivieren Sie die Systemwiederherstellung, falls diese vorhanden ist und genutzt werden soll.

Das Tray Icon zeigt einen deaktivierten Zustand an.

Ursache: Der Avira Echtzeit-Scanner ist deaktiviert.

- Klicken Sie im Control Center **Status** und aktivieren Sie den **Echtzeit-Scanner** im Bereich *PC Sicherheit*.

- ODER -

- Um das Kontextmenü aufzurufen, klicken Sie mit der rechten Maustaste auf das Tray Icon. Klicken Sie **Echtzeit-Scanner einschalten**.

Ursache: Der Avira Echtzeit-Scanner wird von einer Firewall blockiert.

- Definieren Sie in der Konfiguration Ihrer Firewall eine generelle Freigabe für den Avira Echtzeit-Scanner. Der Avira Echtzeit-Scanner arbeitet ausschließlich mit der Adresse 127.0.0.1 (localhost). Es wird keine Verbindung ins Internet aufgebaut. Gleiches gilt für den Avira Email-Schutz.

Ansonsten:

- Überprüfen Sie die Startart des Avira Echtzeit-Scanner Dienstes. Aktivieren Sie ggf. den Dienst: Wählen Sie in der Startleiste **Start > Einstellungen > Systemsteuerung**. Starten Sie das Konfigurationsfenster **Dienste** per Doppelklick (unter Windows XP finden Sie das Dienste-Applet im Unterordner *Verwaltung*). Suchen Sie nach dem Eintrag *Avira Echtzeit-Scanner*. Als Startart muss `Automatisch` eingetragen sein und als Status `Gestartet`. Starten Sie den Dienst ggf. manuell durch Anwählen der entsprechenden Zeile und der Schaltfläche **Starten**. Tritt eine Fehlermeldung auf, überprüfen Sie bitte die Ereignisanzeige.

Der Rechner wird extrem langsam, wenn ich eine Datensicherung durchführe.

Ursache: Der Avira Echtzeit-Scanner durchsucht während des Backup-Prozesses alle Dateien, mit denen die Datensicherung arbeitet.

- Wählen Sie in der Konfiguration **Echtzeit-Scanner > Suche > Ausnahmen** und tragen Sie den Prozessnamen der Backup-Software ein.

Meine Firewall meldet den Avira Echtzeit Scanner und Avira Email-Schutz, sobald diese aktiv sind.

Ursache: Die Kommunikation des Avira Echtzeit-Scanners und Avira Email-Schutzes erfolgt über das Internetprotokoll TCP/IP. Eine Firewall überwacht alle Verbindungen über dieses Protokoll.

- Definieren Sie eine generelle Freigabe für den Avira Echtzeit-Scanner und Avira Email-Schutz. Der Avira Echtzeit-Scanner arbeitet ausschließlich mit der Adresse 127.0.0.1 (localhost). Es wird keine Verbindung ins Internet aufgebaut. Gleiches gilt für den Avira Email-Schutz.

Avira Email-Schutz funktioniert nicht.

Bitte prüfen Sie die Funktionsfähigkeit des Avira Email-Schutzes anhand der folgenden Checklisten, falls in Zusammenhang mit Avira Email-Schutz Probleme auftreten.

Checkliste

- Prüfen Sie, ob Ihr Mail Client sich per Kerberos, APOP oder RPA beim Server anmeldet. Diese Authentifizierungsmethoden werden derzeit nicht unterstützt.
- Prüfen Sie, ob sich Ihr Mail Client per SSL (auch häufig TLS - Transport Layer Security - genannt) am Server anmeldet. Avira Email-Schutz unterstützt kein SSL und beendet daher die SSL verschlüsselte Verbindungen. Falls Sie SSL verschlüsselte Verbindungen ohne Schutz des Avira Email-Schutzes verwenden möchten, müssen Sie für die Verbindung einen anderen Port nutzen als die vom



Email-Schutz überwachten Ports. Die vom Email-Schutz überwachten Ports können in der Konfiguration unter **Email-Schutz > Suche** konfiguriert werden.

- Ist der Avira Email-Schutz Dienst (Service) aktiv? Aktivieren Sie ggf. den Dienst: Wählen Sie in der Startleiste **Start > Einstellungen > Systemsteuerung**. Starten Sie das Konfigurationsfenster **Dienste** per Doppelklick (unter Windows XP finden Sie das Dienste-Applet im Unterordner *Verwaltung*). Suchen Sie nach dem Eintrag *Avira Email-Schutz*. Als Startart muss `Automatisch` eingetragen sein und als Status `Gestartet`. Starten Sie den Dienst ggf. manuell durch Anwählen der entsprechenden Zeile und der Schaltfläche **Starten**. Tritt eine Fehlermeldung auf, überprüfen Sie bitte die Ereignisanzeige. Ist dies nicht von Erfolg gekrönt, sollten Sie ggf. das Avira Produkt über **Start > Einstellungen > Systemsteuerung > Programme ändern oder entfernen** vollständig deinstallieren, den Rechner neu starten und Ihr Avira Produkt anschließend erneut installieren.

Allgemein

Über SSL (Secure Sockets Layer) verschlüsselte POP3 Verbindungen (auch häufig als TLS (Transport Layer Security) bezeichnet) können derzeit nicht geschützt werden und werden ignoriert.

Authentifizierung zum Mail Server wird derzeit nur über Passworte unterstützt. "Kerberos" und "RPA" werden derzeit nicht unterstützt.

Ihr Avira Produkt prüft Emails beim Versenden nicht auf Viren und unerwünschte Programme.

> **Hinweis**
> Wir empfehlen Ihnen, regelmäßig Microsoft Updates durchzuführen, um eventuelle Sicherheitslücken zu schließen.

Eine Email, die über eine TLS-Verbindung versendet wurde, wurde vom Email-Schutz blockiert.

Ursache: Transport Layer Security (TLS: Verschlüsselungsprotokoll für Datenübertragungen im Internet) wird derzeit nicht vom Email-Schutz unterstützt. Sie haben folgende Möglichkeiten die Email zu senden:

- Nutzen Sie einen anderen Port als den von SMTP genutzten Port 25. Sie umgehen damit die Überwachung durch den Email-Schutz.
- Verzichten Sie auf die TLS verschlüsselte Verbindung und deaktivieren Sie die TLS-Unterstützung in Ihrem Email-Client.
- Deaktivieren Sie (vorübergehend) die Überwachung der ausgehenden Emails durch den Email-Schutz in der Konfiguration unter **Email-Schutz > Suche**.

Webchat funktioniert nicht: Chat-Nachrichten werden nicht angezeigt; im Browser werden Daten geladen.

Dieses Phänomen kann bei Chats auftreten, die auf dem HTTP-Protokoll mit 'transfer-encoding: chunked' basieren.

Ursache: Der Browser-Schutz prüft gesendete Daten zunächst vollständig auf Viren und unerwünschte Programme, bevor die Daten im Webbrowser geladen werden. Bei einem Datentransfer mit 'transfer-encoding: chunked' kann der Browser-Schutz die Nachrichtenlänge bzw. die Datenmenge nicht ermitteln.

- Geben Sie in der Konfiguration die URL des Webchats als Ausnahme an (siehe Konfiguration: **Browser-Schutz > Suche > Ausnahmen**).

15.2 Tastaturbefehle

Tastaturbefehle - auch Shortcuts genannt - bieten eine schnelle Möglichkeit durch das Programm zu navigieren, einzelne Module aufzurufen und Aktionen zu starten.

Im Folgenden erhalten Sie eine Übersicht über die verfügbaren Tastaturbefehle. Nähere Hinweise zur Funktionalität und Verfügbarkeit finden Sie im entsprechenden Kapitel der Hilfe.

15.2.1 In Dialogfeldern

Tastaturbefehl	Beschreibung
Strg + Tab **Strg + Bild runter**	Navigation im Control Center Zur nächsten Rubrik wechseln.
Strg + Umsch + Tab **Strg + Bild runter**	Navigation im Control Center Zur vorherigen Rubrik wechseln.
←↑→↓	Navigation in den Konfigurationsrubriken Setzen Sie zunächst den Fokus mit der Maus auf eine Konfigurationsrubrik. Zwischen den Optionen in einem markierten Drop-Down-Listenfeld oder zwischen mehreren Optionen in einer Optionsgruppe wechseln.
Tab	Zur nächsten Option oder Optionsgruppe wechseln.

Umsch + Tab	Zur vorherigen Option oder Optionsgruppe wechseln.
Leertaste	Aktivieren bzw. Deaktivieren eines Kontrollkästchens, wenn die aktive Option ein Kontrollkästchen ist.
Alt + unterstrichener Buchstabe	Option wählen bzw. Befehl ausführen.
Alt + ↓ **F4**	Ausgewähltes Drop-Down-Listenfeld öffnen.
Esc	Ausgewähltes Drop-Down-Listenfeld schließen. Befehl abbrechen und Dialogfeld schließen.
Eingabetaste	Befehl für die aktive Option oder Schaltfläche ausführen.

15.2.2 In der Hilfe

Tastaturbefehl	Beschreibung
Alt + Leertaste	Systemmenü anzeigen.
Alt + Tab	Umschalten zwischen der Hilfe und anderen geöffneten Fenstern.
Alt + F4	Hilfe schließen.
Umschalt + F10	Kontextmenüs der Hilfe anzeigen.
Strg + Tab	Zur nächsten Rubrik im Navigationsfenster wechseln.
Strg + Umsch + Tab	Zur vorherigen Rubrik im Navigationsfenster wechseln.

Bild hoch	Zum Thema wechseln, das oberhalb des aktuellen Themas im Inhaltsverzeichnis, im Index oder in der Liste der Suchergebnisse angezeigt wird.
Bild runter	Zum Thema wechseln, das unterhalb des aktuellen Themas im Inhaltsverzeichnis, im Index oder in der Liste der Suchergebnisse angezeigt wird.
Bild hoch **Bild runter**	Durch ein Thema blättern.

15.2.3 Im Control Center

Allgemein

Tastaturbefehl	Beschreibung
F1	Hilfe anzeigen
Alt + F4	Control Center schließen
F5	Ansicht aktualisieren
F8	Konfiguration öffnen
F9	Update starten

Rubrik **System-Scanner**

Tastaturbefehl	Beschreibung
F2	Ausgewähltes Profil umbenennen
F3	Suchlauf mit dem ausgewählten Profil starten
F4	Desktopverknüpfung für das ausgewählte Profil erstellen
Einf	Neues Profil erstellen



Entf	Ausgewähltes Profil löschen

Rubrik **Quarantäne**

Tastaturbefehl	Beschreibung
F2	Objekt erneut prüfen
F3	Objekt wiederherstellen
F4	Objekt senden
F6	Objekt wiederherstellen nach...
Enter	Eigenschaften
Einf	Datei hinzufügen
Entf	Objekt löschen

Rubrik **Planer**

Tastaturbefehl	Beschreibung
F2	Auftrag ändern
Enter	Eigenschaften
Einf	Neuen Auftrag einfügen
Entf	Auftrag löschen

Rubrik **Berichte**

Tastaturbefehl	Beschreibung
F3	Reportdatei anzeigen
F4	Reportdatei drucken
Enter	Bericht anzeigen
Entf	Bericht(e) löschen

Rubrik **Ereignisse**

Tastaturbefehl	Beschreibung
F3	Ereignis(se) exportieren
Enter	Ereignis anzeigen
Entf	Ereignis(se) löschen

15.3 Windows Sicherheitscenter

- Windows XP Service Pack 3 -

15.3.1 Allgemeines

Das Windows Sicherheitscenter überprüft den Status eines Computers im Hinblick auf wichtige Sicherheitsaspekte.

Wenn bei einem dieser wichtigen Punkte ein Problem festgestellt wird (z.B. ein veraltetes Antivirenprogramm), sendet das Sicherheitscenter eine Warnung und stellt Empfehlungen bereit, wie Sie den Computer besser schützen können.

15.3.2 Das Windows Sicherheitscenter und Ihr Avira Produkt

Virenschutzsoftware / Schutz vor schädlicher Software

Folgende Hinweise können Sie in Bezug auf Ihren Virenschutz vom Windows Sicherheitscenter erhalten.

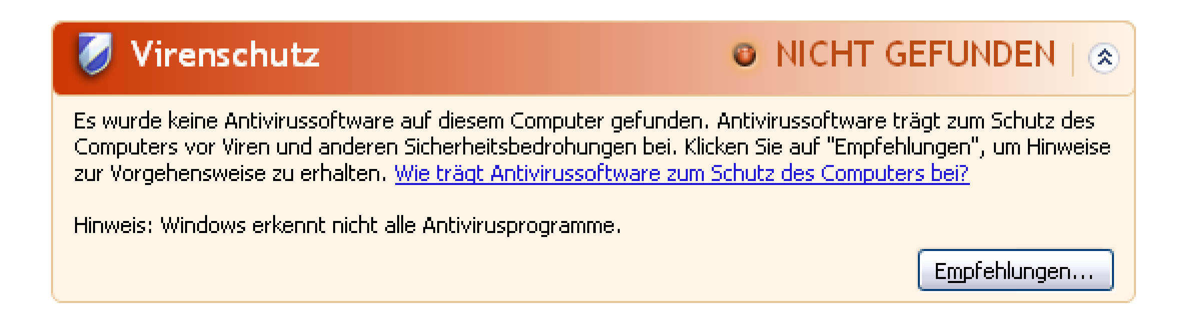
- Virenschutz NICHT GEFUNDEN



- Virenschutz NICHT AKTUELL
- Virenschutz AKTIV
- Virenschutz INAKTIV
- Virenschutz NICHT ÜBERWACHT

Virenschutz NICHT GEFUNDEN

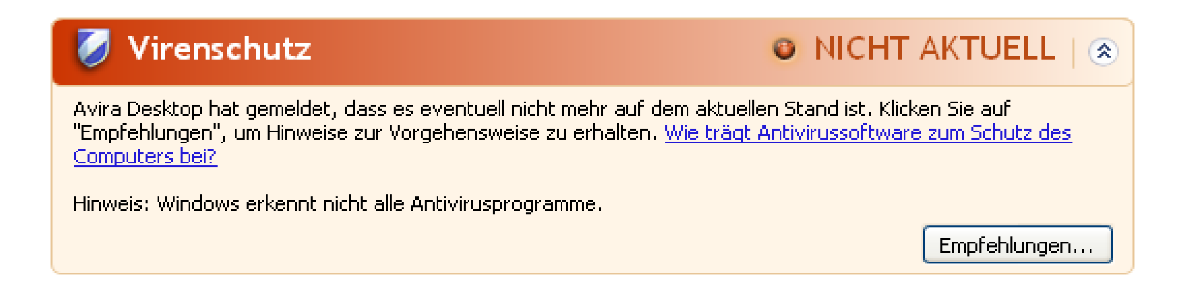
Dieser Hinweis des Windows Sicherheitscenters erscheint, wenn das Windows Sicherheitscenter keine Antivirensoftware auf Ihrem Computer gefunden hat.



Hinweis
Installieren Sie Ihr Avira Produkt auf Ihrem Computer, um diesen vor Viren und sonstigen unerwünschten Programmen zu schützen!

Virenschutz NICHT AKTUELL

Haben Sie Windows XP Service Pack 3 bereits installiert und installieren danach Ihr Avira Produkt oder aber installieren Sie Windows XP Service Pack 3 auf ein System, auf dem Ihr Avira Produkt bereits installiert war erhalten Sie folgende Meldung:

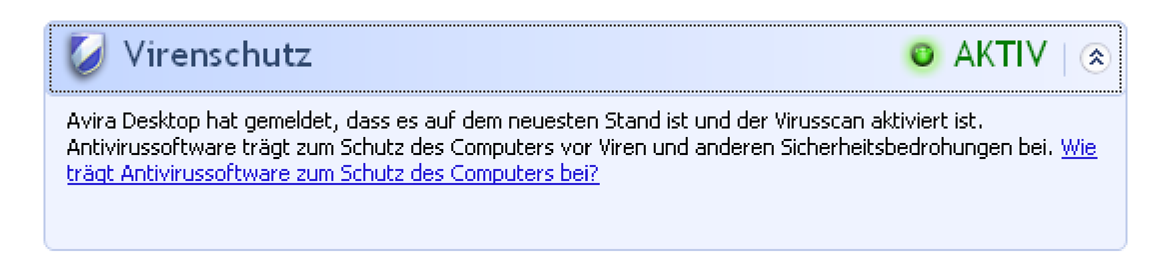


Hinweis
Damit das Windows Sicherheitscenter Ihr Avira Produkt als aktuell erkennt, ist nach der Installation zwingend ein Update erforderlich. Sie aktualisieren Ihr System, indem Sie ein Update durchführen.



Virenschutz AKTIV

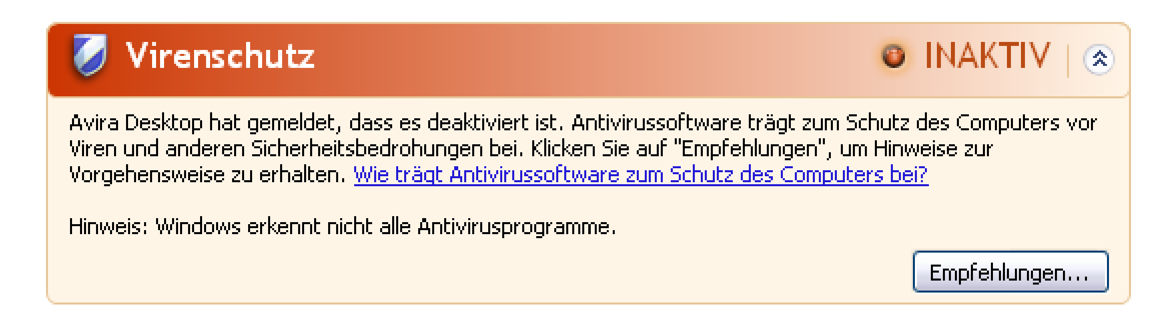
Nach der Installation Ihres Avira Produkts und einem im Anschluss daran durchgeführten Update erhalten Sie folgenden Hinweis:



Ihr Avira Produkt ist nun auf aktuellem Stand und der Avira Echtzeit-Scanner ist aktiv.

Virenschutz INAKTIV

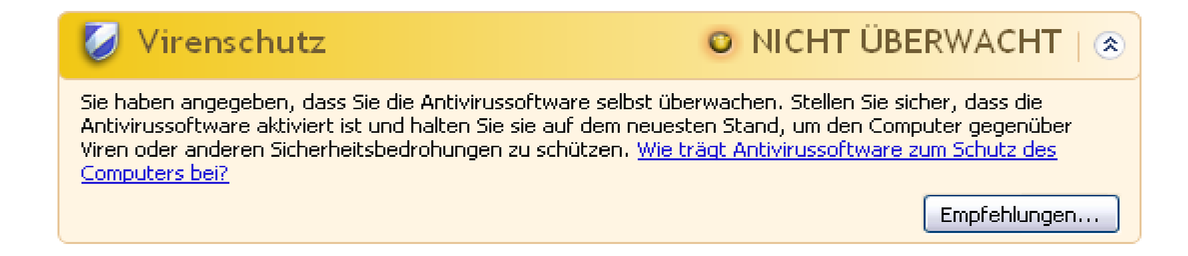
Nachfolgenden Hinweis erhalten Sie, wenn Sie den Avira Echtzeit-Scanner deaktivieren oder aber den Echtzeit-Scanner Dienst stoppen.



Hinweis
Den Avira Echtzeit-Scanner können Sie unter der Rubrik **Status** des **Control Centers** aktivieren bzw. deaktivieren. Sie erkennen zudem, dass der Avira Echtzeit-Scanner aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist.

Virenschutz NICHT ÜBERWACHT

Erhalten Sie folgenden Hinweis vom Windows Sicherheitscenter, dann haben Sie sich dafür entschieden, dass Sie Ihre Antivirensoftware selbst überwachen.





> **Hinweis**
> Das Windows Sicherheitscenter wird von Ihrem Avira Produkt unterstützt. Sie können diese Option jederzeit über die Schaltfläche **Empfehlungen...** aktivieren.

> **Hinweis**
> Auch wenn Sie Windows XP Service Pack 3 installiert haben benötigen Sie weiterhin eine Virenschutzlösung. Obwohl Windows Ihre Antivirensoftware überwacht, enthält es selbst keinerlei Antivirus-Funktionen. Sie wären also ohne eine zusätzliche Virenschutzlösung nicht vor Viren und sonstiger Malware geschützt!

15.4 Windows Wartungscenter

- Windows 7 und Windows 8 -

15.4.1 Allgemein

> **Hinweis:**
> Das **Windows Sicherheitscenter** wurde ab Windows 7 in **Windows Wartungscenter** umbenannt. Unter diesem Programmabschnitt finden Sie jetzt den Status aller Ihrer Sicherheits-Optionen.

Das Windows Wartungscenter überprüft den Status eines Computers im Hinblick auf wichtige Sicherheitsaspekte. Sie können direkt auf das Wartungscenter zugreifen, indem Sie auf die kleine Flagge in Ihrer Taskleiste klicken oder unter **Systemsteuerung > Wartungscenter**.

Wenn bei einem dieser wichtigen Punkte ein Problem festgestellt wird (z.B. ein veraltetes Antivirenprogramm), sendet das Wartungscenter eine Warnung und stellt Empfehlungen bereit, wie Sie den Computer besser schützen können. Das bedeutet, wenn alles richtig funktioniert, werden Sie keine Meldung vom Wartungscenter erhalten. Trotzdem ist es möglich, den Sicherheitsstatus des Computers im **Wartungscenter** unter der Rubrik **Sicherheit** zu beobachten.
Das **Windows Wartungscenter** bietet Ihnen auch die Möglichkeit, die Programme, die Sie installiert haben, zu verwalten und auszuwählen (z.B. *Antispywareprogramme auf dem Computer anzeigen*).

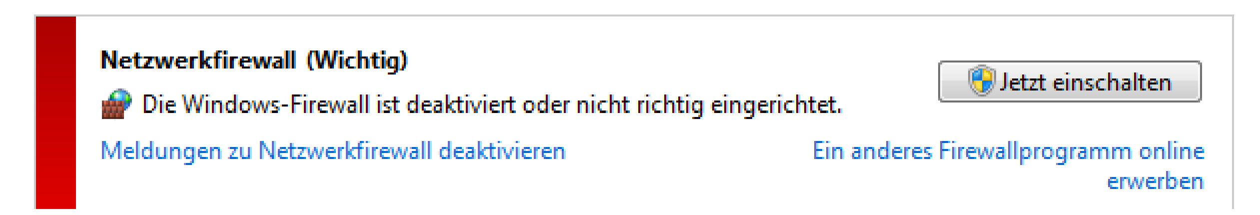
Sie können die Warnmeldungen unter **Wartungscenter > Einstellungen ändern** (z.B. *Meldungen zum Schutz vor Spyware und ähnlicher Malware deaktivieren*) ausschalten.



15.4.2 Das Windows Wartungscenter und Ihr Avira Produkt

- Die Windows-Firewall ist deaktiviert oder nicht richtig eingerichtet

Die Windows-Firewall ist deaktiviert oder nicht richtig eingerichtet



- **Windows Firewall ist installiert**

  Ab Windows 7 ist Avira FireWall in Avira Antivirus Suite nicht mehr enthalten. Sie haben stattdessen die Möglichkeit, die Windows-Firewall mithilfe des Control- und Konfigurationscenters zu steuern.

Virenschutz

Folgende Hinweise können Sie in Bezug auf Ihren Virenschutz vom Windows Wartungscenter erhalten:

- Avira Desktop meldet, dass es auf dem neuesten Stand ist und die Virenerkennung eingeschaltet ist.
- Avira Desktop ist deaktiviert.
- Avira Desktop ist nicht mehr aktuell.
- Es wurde keine Antivirensoftware auf dem Computer gefunden.

Avira Desktop meldet, dass es auf dem neuesten Stand ist und die Virenerkennung eingeschaltet ist

Nach der Installation Ihres Avira Produkts und einem im Anschluss daran durchgeführten Update werden Sie zunächst keine Meldungen vom Windows Wartungscenter erhalten. Sie können jedoch unter **Wartungscenter > Sicherheit** folgenden Hinweis finden: *Avira Desktop meldet, dass es auf dem neuesten Stand ist und die Virenerkennung eingeschaltet ist.* Das heißt, dass Ihr Avira Produkt auf aktuellem Stand ist und der Avira Echtzeit-Scanner aktiv ist.

Avira Desktop meldet, dass es deaktiviert ist

Nachfolgenden Hinweis erhalten Sie, wenn Sie den Avira Echtzeit-Scanner deaktivieren oder aber den Echtzeit-Scanner Dienst stoppen.



Virenschutz (Wichtig)
Avira Desktop ist deaktiviert.
Meldungen zu Virenschutz deaktivieren
Jetzt einschalten
Ein anderes Antivirenprogramm online erwerben

> **Hinweis**
> Den Avira Echtzeit-Scanner können Sie unter der Rubrik **Status** des **Avira Control Centers** aktivieren bzw. deaktivieren. Sie können zudem erkennen, ob der Avira Echtzeit-Scanner aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist. Es ist auch möglich, die einzelnen Avira Komponenten durch das Anklicken der *Jetzt einschalten*-Taste des Wartungscenters zu aktivieren. Sie werden eine Meldung erhalten, um Ihre Zustimmung zum Ausführen des Avira Programms zu geben. Klicken Sie *Ja, ich vertraue dem Herausgeber und möchte das Programm ausführen*, dann wird der Echtzeit-Scanner wieder aktiviert.

Avira Desktop ist nicht mehr aktuell

Wenn Sie gerade Avira installiert haben, oder wenn aus irgendeinem Grund die Virendefinitionsdatei, die Suchengine oder die Programmdateien Ihres Avira Produkts nicht automatisch aktualisiert wurden (z.B. wenn Sie von einer älteren Version eines Windows Betriebssystems, auf dem Ihr Avira Produkt bereits installiert ist, auf eine neuere Version upgraden), erhalten Sie folgende Meldung:

Virenschutz (Wichtig)
"Avira Desktop" ist nicht mehr aktuell.
Meldungen zu Virenschutz deaktivieren
Jetzt aktualisieren
Ein anderes Antivirenprogramm online erwerben

> **Hinweis**
> Damit das Windows Wartungscenter Ihr Avira Produkt als aktuell erkennt, ist nach der Installation zwingend ein Update erforderlich. Sie aktualisieren Ihr System, indem Sie ein Update durchführen.

Es wurde keine Antivirensoftware auf dem Computer gefunden

Dieser Hinweis des Windows Wartungscenters erscheint, wenn das Windows Wartungscenter keine Antivirensoftware auf Ihrem Computer gefunden hat.

Virenschutz (Wichtig)
Es wurde keine Antivirensoftware auf dem Computer gefunden.
Meldungen zu Virenschutz deaktivieren

Programm online suchen

Hinweis
Bitte beachten Sie, dass diese Option nicht in Windows 8 verfügbar ist. Windows Defender ist ab diesem Betriebssystem die von Microsoft voreingestellte Virenschutzfunktion.

Hinweis
Installieren Sie Ihr Avira Produkt auf Ihrem Computer, um diesen vor Viren und sonstigen unerwünschten Programmen zu schützen!

Schutz vor Spyware und unerwünschter Software

Folgende Hinweise können Sie in Bezug auf Ihren Schutz vor Spyware und unerwünschter Software vom Windows Wartungscenter erhalten:

- Avira Desktop gemeldet, dass es eingeschaltet ist.
- Sowohl Windows Defender als auch Avira Desktop haben gemeldet, dass sie ausgeschaltet sind.
- Avira Desktop ist nicht mehr aktuell.
- Windows Defender ist nicht mehr aktuell.
- Windows Defender ist ausgeschaltet.

Avira Desktop hat gemeldet, dass es eingeschaltet ist

Nach der Installation Ihres Avira Produkts und einem im Anschluss daran durchgeführten Update werden Sie zunächst keine Meldungen vom Windows Wartungscenter erhalten. Sie können jedoch unter **Wartungscenter > Sicherheit** folgenden Hinweis finden: *"Avira Desktop" hat gemeldet, dass es eingeschaltet ist*. Das heißt, dass Ihr Avira Produkt auf aktuellem Stand ist und der Avira Echtzeit-Scanner aktiv ist.

Sowohl Windows Defender als auch Avira Desktop haben gemeldet, dass sie ausgeschaltet sind

Nachfolgenden Hinweis erhalten Sie, wenn Sie den Avira Echtzeit-Scanner deaktivieren oder aber den Echtzeit-Scanner Dienst stoppen.

Schutz vor Spyware und unerwünschter Software (Wichtig)
Sowohl Windows Defender als auch Avira Desktop haben gemeldet, dass sie ausgeschaltet sind.
Meldungen zu Schutz vor Spyware und ähnlicher Malware deaktivieren
Antispywareprogramme anzeigen

Hinweis
Den Avira Echtzeit-Scanner können Sie unter der Rubrik **Status** des **Avira Control Centers** aktivieren bzw. deaktivieren. Sie können zudem erkennen, ob der Avira Echtzeit-Scanner aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist. Es ist auch möglich, die einzelnen Avira Komponenten durch das Anklicken der *Jetzt einschalten*-Taste des Wartungscenters zu aktivieren. Sie werden eine Meldung erhalten, um Ihre Zustimmung zum Ausführen des Avira Programms zu geben. Klicken Sie *Ja, ich vertraue dem Herausgeber und möchte das Programm ausführen*, dann wird der Echtzeit-Scanner wieder aktiviert.

Avira Desktop ist nicht mehr aktuell

Wenn Sie gerade Avira installiert haben, oder wenn aus irgendeinem Grund die Virendefinitionsdatei, die Suchengine oder die Programmdateien Ihres Avira Produkts nicht automatisch aktualisiert wurden (z.B. wenn Sie von einer älteren Version eines Windows Betriebssystems, auf dem Ihr Avira Produkt bereits installiert ist, auf eine neuere Version upgraden), erhalten Sie folgende Meldung:

Schutz vor Spyware und unerwünschter Software (Wichtig)
"Avira Desktop" ist nicht mehr aktuell.
Meldungen zu Schutz vor Spyware und ähnlicher Malware deaktivieren
Jetzt aktualisieren
Ein anderes Antispywareprogramm online erwerben

Hinweis
Damit das Windows Wartungscenter Ihr Avira Produkt als aktuell erkennt, ist nach der Installation zwingend ein Update erforderlich. Sie aktualisieren Ihr System, indem Sie ein Update durchführen.

Windows Defender ist nicht mehr aktuell

Die folgende Meldung kann angezeigt werden, wenn Windows Defender aktiviert ist. Das könnte bedeuten, dass Ihr Avira Produkt nicht richtig installiert wurde. Bitte überprüfen Sie dies.



Schutz vor Spyware und unerwünschter Software (Wichtig)
Windows Defender ist nicht mehr aktuell.
Jetzt aktualisieren
Meldungen zu Schutz vor Spyware und ähnlicher Malware deaktivieren
Ein anderes Antispywareprogramm online erwerben

Hinweis
Windows Defender ist die vordefinierte Spyware- und Virenschutz-Lösung von Windows.

Windows Defender ist ausgeschaltet

Sie erhalten die Meldung des Windows Wartungscenters Windows Defender ist ausgeschaltet, wenn keine andere Antispyware-Software auf Ihrem Computer gefunden wurde. Windows Defender ist eine von Microsoft im Betriebssystem standardmäßig integrierte Software zur Erkennung von Spyware. Wenn Sie schon eine andere Antivirensoftware auf Ihrem Computer installiert hatten, wurde diese Anwendung deaktiviert. Ist das Avira Produkt richtig installiert, sollten Sie diese Meldung nicht erhalten, denn das Wartungscenter erkennt Avira automatisch. Bitte überprüfen Sie dies.

Schutz vor Spyware und unerwünschter Software (Wichtig)
Windows Defender ist ausgeschaltet.
Jetzt einschalten
Meldungen zu Schutz vor Spyware und ähnlicher Malware deaktivieren
Ein anderes Antispywareprogramm online erwerben

16. Viren und mehr

Avira Antivirus Suite erkennt nicht nur Viren und Malware, das Produkt kann Sie auch vor weiteren Gefahren schützen. In diesem Kapitel finden Sie einen Überblick über die verschiedenen Arten von Malware sowie über andere Gefahren. Dieser beschreibt sowohl woher sie kommen und ihr Verhalten als auch die unliebsamen Überraschungen, die damit auf Sie zukommen.

Verwandte Themen:

- Gefahrenkategorien
- Viren sowie sonstige Malware

16.1 Gefahrenkategorien

Adware

Als Adware wird Software bezeichnet, die dem Benutzer zusätzlich zur eigentlichen Funktionalität Werbe-Banner oder Werbe-Popups zeigt. Diese Werbeeinblendungen lassen sich in der Regel nicht abschalten und sind meist immer sichtbar. Hier erlauben die Verbindungsdaten bereits vielfältige Rückschlüsse auf das Nutzungsverhalten und sind aus Datenschutzgründen problematisch.

Ihr Avira Produkt erkennt Adware. Ist in der Konfiguration unter Gefahrenkategorien die Option **Adware** aktiviert, erhalten Sie eine entsprechende Warnmeldung, wenn Ihr Avira Produkt solche Software entdeckt.

Adware/Spyware

Software, die Werbung einblendet oder Software, die persönliche Daten des Anwenders häufig ohne dessen Wissen oder Zustimmung an Dritte versendet und daher möglicherweise unerwünscht ist.

Ihr Avira Produkt erkennt "Adware/Spyware". Ist in der Konfiguration unter Gefahrenkategorien die Option **Adware/Spyware** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Anwendung

Bei der Bezeichnung Anwendung handelt es sich um eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.
Ihr Avira Produkt erkennt "Anwendung" (APPL). Ist in der Konfiguration unter Gefahrenkategorien die Option **Anwendung** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt ein solches Verhalten bemerkt.

Backdoor-Steuersoftware

Um Daten zu stehlen oder Rechner zu manipulieren, wird "durch die Hintertür" ein Backdoor-Server-Programm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder Netzwerk kann dieses Programm über eine Backdoor-Steuersoftware (Client) von Dritten gesteuert werden.
Ihr Avira Produkt erkennt "Backdoor-Steuersoftware". Ist in der Konfiguration unter Gefahrenkategorien die Option **Backdoor-Steuersoftware** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Dateien mit verschleierten Dateiendungen

Ausführbare Dateien, die ihre wahre Dateiendung in verdächtiger Weise verschleiern. Diese Methode der Verschleierung wird häufig von Malware benutzt.
Ihr Avira Produkt erkennt "Dateien mit verschleierten Dateiendungen". Ist in der Konfiguration unter Gefahrenkategorien die Option **Dateien mit verschleierten Dateiendungen** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Kostenverursachendes Einwahlprogramm

Bestimmte im Internet angebotene Dienstleistungen sind kostenpflichtig. Die Abrechnung erfolgt in Deutschland über Einwahlprogramme mit 0190/0900-Nummern (in Österreich und der Schweiz über 09x0-Nummern; in Deutschland wird mittelfristig auf 09x0 umgestellt). Auf dem Rechner installiert, gewährleisten diese Programme - kurz Dialer genannt - den Verbindungsaufbau über eine entsprechende Premium-Rate-Nummer, deren Tarifgestaltung ein breites Spektrum umfassen kann.

Die Vermarktung von Online-Inhalten über den Weg der Telefonrechnung ist legal und kann für den Nutzer vorteilhaft sein. Seriöse Dialer lassen deshalb keinen Zweifel daran aufkommen, dass sie vom Kunden bewusst und mit Bedacht eingesetzt werden. Sie installieren sich nur dann auf dem Anwender-Rechner, wenn der Nutzer dazu seine Zustimmung abgibt, wobei diese Zustimmung aufgrund einer völlig eindeutigen und klar erkennbaren Etikettierung bzw. Aufforderung erfolgt sein muss. Der Verbindungsaufbau seriöser Dialer-Programme wird unmissverständlich angezeigt. Außerdem informieren seriöse Dialer exakt und augenfällig über die Höhe der dabei entstehenden Kosten.

Leider jedoch gibt es Dialer, die sich unauffällig, auf fragwürdige Weise oder gar in betrügerischer Absicht auf Rechnern installieren. Sie ersetzen z.B. die Standard-DFÜ-Verbindung des Internet-Nutzers zum ISP (Internet-Service-Provider) und rufen bei jeder Verbindung eine kostenverursachende, oft horrend überteuerte 0190/0900-Nummer an. Der betroffene Anwender merkt mitunter erst mit der nächsten Telefonrechnung, dass ein unerwünschtes 0190/0900-Dialer-Programm auf seinem Rechner bei jedem Verbindungsaufbau zum Internet eine Premium-Rate-Nummer gewählt hat - mit der Folge drastisch hoher Gebühren.

Um sich generell vor unerwünschten kostenverursachenden Einwahlprogrammen (0190/0900-Dialern) zu schützen, empfehlen wir Ihnen, sich direkt bei Ihrem Telefon-Anbieter für diesen Nummernkreis sperren zu lassen.

Standardmäßig erkennt Ihr Avira Produkt die ihm bekannten kostenverursachende Einwahlprogramme.

Ist in der Konfiguration unter Gefahrenkategorien die Option **Kostenverursachendes Einwahlprogramm** mit einem Häkchen aktiviert, erhalten Sie bei Auffinden eines kostenverursachenden Einwahlprogramms einen entsprechenden Warnhinweis. Sie haben nun die Möglichkeit, den eventuell unerwünschten 0190/0900-Dialer einfach zu löschen. Ist dies allerdings ein erwünschtes Einwahlprogramm, können Sie es als Ausnahmedatei deklarieren und diese Datei wird dann zukünftig nicht mehr untersucht.

Phishing

Phishing, auch bekannt als "brand spoofing" ist eine raffinierte Form des Datendiebstahls, der auf Kunden bzw. potienzielle Kunden von Internet Service Providern, Banken, Online-Banking Diensten, Registrierungsbehörden abzielt.
Durch eine Weitergabe der eigenen Email-Adresse im Internet, das Ausfüllen von Online-Formularen, dem Beitritt von Newsgroups oder Webseiten ist es möglich, dass Ihre Daten von sog. "Internet crawling spiders" gestohlen und ohne Ihre Erlaubnis dazu verwendet werden einen Betrug oder andere Verbrechen zu begehen.

Ihr Avira Produkt erkennt "Phishing". Ist in der Konfiguration unter Gefahrenkategorien die Option **Phishing** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt ein solches Verhalten bemerkt.

Programme, die die Privatsphäre verletzen

Software, die die Sicherheit Ihres Systems beeinträchtigen, nicht gewünschte Programmaktivitäten auslösen, Ihre Privatsphäre verletzen oder Ihr Benutzerverhalten ausspähen kann und daher möglicherweise unerwünscht ist.

Ihr Avira Produkt erkennt "Security Privacy Risk" Software. Ist in der Konfiguration unter Gefahrenkategorien die Option **Programme, die die Privatsphäre verletzen** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Scherzprogramme

Die Scherzprogramme sollen lediglich jemanden erschrecken oder zur allgemeinen Belustigung dienen, ohne schädlich zu sein oder sich selbst zu vermehren. Meist fängt der Computer nach dem Aufruf eines Witzprogramms irgendwann an, eine Melodie zu spielen oder etwas Ungewohntes auf dem Bildschirm zu zeigen. Beispiele für Witzprogramme sind die Waschmaschine im Diskettenlaufwerk (DRAIN.COM) und der Bildschirmfresser (BUGSRES.COM).

Aber Vorsicht! Alle Symptome von Scherzprogrammen könnten auch von einem Virus oder einem Trojaner stammen. Zumindest bekommt man aber einen gehörigen Schreck oder richtet in Panik hinterher sogar selbst tatsächlichen Schaden an.

Ihr Avira Produkt ist in der Lage, durch die Erweiterung seiner Such- und Identifikationsroutinen Witzprogramme zu erkennen und sie als unerwünschtes Programm ggf. zu eliminieren. Ist in der Konfiguration unter Gefahrenkategorien die Option **Scherzprogramme** mit einem Häkchen aktiviert, wird über entsprechende Funde informiert.

Spiele

Computerspiele müssen sein - aber sie gehören nicht unbedingt an den Arbeitsplatz (die Mittagspause vielleicht einmal ausgenommen). Dennoch wird von Mitarbeitern in Unternehmen und Behörden so manches Moorhuhn erlegt und so mancher Karobube doppelgeklickt. Über das Internet kann eine Fülle von Spielen heruntergeladen werden. Auch Email-Games erfreuen sich wachsender Verbreitung: Vom simplen Schach bis zum "Flottenmanöver" (inklusive Torpedogefecht) sind zahlreiche Varianten in Umlauf: Die jeweiligen Spielzüge werden über Mailprogramme an Partner gesendet und von diesen beantwortet.

Untersuchungen haben ergeben, dass die zum Computerspielen verwendete Arbeitszeit längst wirtschaftlich relevante Größenordnungen erreicht hat. Umso verständlicher ist, dass immer mehr Unternehmen Möglichkeiten in Betracht ziehen, Computerspiele von Arbeitsplatzrechnern fern zu halten.

Ihr Avira Produkt erkennt Computerspiele. Ist in der Konfiguration unter Gefahrenkategorien die Option **Spiele** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist. Das Spiel ist nun im wahrsten Sinne des Wortes aus, denn Sie haben die Möglichkeit, es einfach zu löschen.

Trügerische Software

Auch als "Scareware" (Schreckprogramme) oder "Rogueware" (Schurkenprogramme) bekannt, bezeichnet betrügerische Software, die Vireninfektionen und Gefahren vorgaukelt und dabei professioneller Antivirensoftware täuschend ähnlich sieht. Scareware ist darauf ausgelegt, den Benutzer zu verunsichern oder zu verängstigen. Fällt das Opfer auf den Trick herein und glaubt sich bedroht, wird ihm häufig gegen Bezahlung eine Beseitigung der nicht vorhandenen Gefahr angeboten. In anderen Fällen soll das Opfer durch den Glauben an einen erfolgreichen Angriff zu Handlungen verleitet werden, welche einen tatsächlichen Angriff erst ermöglichen.

Ist in der Konfiguration unter Gefahrenkategorien die Option **Trügerische Software** mit einem Häkchen aktiviert, erhalten Sie bei Auffinden von Scareware einen entsprechenden Warnhinweis.

Ungewöhnliche Laufzeitpacker

Dateien, die mit einem ungewöhnlichen Laufzeitpacker komprimiert wurden und daher als möglicherweise verdächtig eingestuft werden können.

Ihr Avira Produkt erkennt "Ungewöhnliche Laufzeitpacker". Ist in der Konfiguration unter Gefahrenkategorien die Option **Ungewöhnliche Laufzeitpacker (PCK)** aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

16.2 Viren sowie sonstige Malware

Adware

Als Adware wird Software bezeichnet, die dem Benutzer zusätzlich zur eigentlichen Funktionalität Werbe-Banner oder Werbe-Popups zeigt. Diese Werbeeinblendungen lassen sich in der Regel nicht abschalten und sind meist immer sichtbar. Hier erlauben die Verbindungsdaten bereits vielfältige Rückschlüsse auf das Nutzungsverhalten und sind aus Datenschutzgründen problematisch.

Backdoors

Einem Backdoor (deutsch: Hintertür) ist es möglich, unter Umgehung der Zugriffssicherung, Zugriff auf einen Computer zu erlangen.

Ein versteckt laufendes Programm ermöglicht einem Angreifer meist fast uneingeschränkte Rechte. Mit Hilfe des Backdoors können persönliche Daten des Anwenders ausspioniert werden. Aber Sie werden meist dazu benutzt, weitere Computerviren oder Würmer auf dem betroffenen System zu installieren.

Bootviren

Der Boot- bzw. Masterbootsektor von Festplatten wird mit Vorliebe von Bootsektorviren infiziert. Sie überschreiben wichtige Informationen zum Systemstart. Eine der unangenehmen Folgen: das Betriebssystem kann nicht mehr geladen werden…

Bot-Net

Unter einem Bot-Net versteht man ein fernsteuerbares Netzwerk (im Internet) von PCs, welches aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Viren bzw. Trojaner erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Diese Netzwerke können für Spam-Verbreitung, DDoS Attacken, usw. verwendet werden, z.T. ohne dass die betroffenen PC-Nutzer etwas merken. Das Hauptpotenzial von Bot-Nets besteht darin, dass die Netzwerke Größen von tausenden Rechnern erreichen können, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge sprengt.

Exploit

Ein Exploit (Sicherheitslücke) ist ein Computerprogramm oder Script, welches spezifische Schwächen oder Fehlfunktionen eines Betriebssystems oder Programms ausnutzt. Eine Form des Exploits sind Angriffe aus dem Internet mit Hilfe von manipulierten Datenpaketen, die Schwachstellen in der Netzwerksoftware ausnutzen. Hier können Programme eingeschleust werden, mit denen ein größerer Zugriff erlangt werden kann.

Phishing

Auch als "Scareware" (Schreckprogramme) oder "Rogueware" (Schurkenprogramme) bekannt, bezeichnet betrügerische Software, die Vireninfektionen und Gefahren vorgaukelt. Dabei sieht sie professioneller Antivirensoftware täuschend ähnlich. Scareware ist darauf ausgelegt, den Benutzer zu verunsichern oder zu verängstigen. Fällt das Opfer auf den Trick herein und glaubt sich bedroht, wird ihm häufig gegen Bezahlung eine Beseitigung der nicht vorhandenen Gefahr angeboten. In anderen Fällen soll das Opfer durch den Glauben an einen erfolgreichen Angriff zu Handlungen verleitet werden, welche einen tatsächlichen Angriff erst ermöglichen.

Hoaxes

Seit ein paar Jahren erhalten die User im Internet und in anderen Netzen Warnungen vor Viren, die sich angeblich per Email verbreiten sollen. Diese Warnungen werden über Email mit der Aufforderung verbreitet, sie an möglichst viele Kollegen und andere Benutzer weiter zu senden, um alle vor der "Gefahr" zu warnen.

Honeypot

Ein Honeypot (Honigtopf) ist ein in einem Netzwerk installierter Dienst (Programm oder Server). Dieser hat die Aufgabe, ein Netzwerk zu überwachen und Angriffe zu protokollieren. Dieser Dienst ist dem legitimen Nutzer unbekannt und wird daher niemals angesprochen. Wenn nun ein Angreifer ein Netzwerk auf Schwachstellen untersucht und dabei die von einem Honeypot angebotenen Dienste in Anspruch nimmt, wird er protokolliert und ein Alarm ausgelöst.

Makroviren

Makroviren sind kleine Programme, die in der Makrosprache einer Anwendung (z.B. WordBasic unter WinWord 6.0) geschrieben sind und sich normalerweise auch nur innerhalb von Dokumenten dieser Anwendung verbreiten können. Sie werden deshalb auch Dokumentviren genannt. Damit sie aktiv werden, sind sie immer darauf angewiesen, dass die entsprechende Applikation gestartet und eines der infizierten Makros ausgeführt wird. Im Unterschied zu "normalen" Viren befallen Makroviren also keine ausführbaren Dateien sondern die Dokumente der jeweiligen Wirts-Applikation.

Pharming

Pharming ist eine Manipulation der Hostdatei von Webbrowsern, um Anfragen auf gefälschte Webseiten umzuleiten. Es handelt sich um eine Weiterentwicklung des klassischen Phishings. Pharming-Betrüger unterhalten eigene große Server-Farmen, auf denen gefälschte Webseiten abgelegt sind. Pharming hat sich auch als Oberbegriff für verschiedene Arten von DNS-Angriffen etabliert. Bei einer Manipulation der Host-Datei wird unter Zuhilfenahme eines Trojaners oder eines Virus eine gezielte Manipulation des Systems vorgenommen. Die Folge davon ist, dass von diesem System nur noch gefälschte Websites abrufbar sind, selbst wenn die Web-Adresse korrekt eingegeben wurde.

Spiele

Phishing bedeutet ins Deutsche übersetzt das Fischen nach persönlichen Daten des Internetnutzers. Der Phisher schickt seinem Opfer in der Regel offiziell wirkende Schreiben, wie beispielsweise Emails, die es verleiten sollen, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, im guten Glauben dem Täter preiszugeben. Mit den gestohlenen Zugangsdaten kann der Phisher die Identität seines Opfers übernehmen und in dessen Namen Handlungen ausführen. Klar ist: Banken und Versicherungen bitten niemals um die Zusendung von Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per Email, per SMS oder telefonisch.

Polymorphe Viren

Polymorphe Viren sind wahre Meister der Tarnung und Verkleidung. Sie verändern ihre eigenen Programmiercodes - und sind deshalb besonders schwer zu erkennen.

Programmviren

Ein Computervirus ist ein Programm, das die Fähigkeit besitzt, sich nach seinem Aufruf selbsttätig an andere Programme auf irgendeine Weise anzuhängen und dadurch zu infizieren. Viren vervielfältigen sich also im Gegensatz zu logischen Bomben und Trojanern selber. Im Gegensatz zu einem Wurm benötigt der Virus immer ein fremdes Programm als Wirt, in dem er seinen virulenten Code ablegt. Im Normalfall wird aber der eigentliche Programmablauf des Wirtes selber nicht geändert.

Rootkits

Unter Rootkits versteht man eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem installiert werden, um Logins des Eindringlings zu verbergen, Prozesse zu verstecken und Daten mitzuschneiden - generell gesagt: sich unsichtbar zu machen. Sie versuchen bereits installierte Spionageprogramme zu aktualisieren und gelöschte Spyware erneut zu installieren.



Skriptviren und Würmer

Diese Viren sind extrem einfach zu programmieren und verbreiten sich - entsprechende Techniken vorausgesetzt - innerhalb weniger Stunden per Email um den ganzen Erdball.

Skriptviren und -würmer benutzen eine der Script-Sprachen, wie beispielsweise Javascript, VBScript etc., um sich selbst in andere, neue Skripte einzufügen oder sich selber durch den Aufruf von Betriebssystemfunktionen zu verbreiten. Häufig geschieht dies per Email oder durch den Austausch von Dateien (Dokumenten).

Als Wurm wird ein Programm bezeichnet, das sich selber vervielfältigt jedoch keinen Wirt infiziert. Würmer können also nicht Bestandteil anderer Programmabläufe werden. Würmer sind auf Systemen mit restriktiveren Sicherheitsvorkehrungen oft die einzige Möglichkeit irgendwelche Schadensprogramme einzuschleusen.

Spyware

Spyware sind sogenannte Spionageprogramme, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte sendet. Meist dienen Spyware-Programme dazu, das Surf-Verhalten im Internet zu analysieren und gezielte Werbe-Banner oder Werbe-Popups einzublenden.

Trojanische Pferde (kurz Trojaner)

Trojaner sind in letzter Zeit recht häufig anzutreffen. So bezeichnet man Programme, die vorgeben, eine bestimmte Funktion zu haben, nach ihrem Start aber ihr wahres Gesicht zeigen und irgendeine andere Funktion ausführen, die zumeist zerstörerisch ist. Trojanische Pferde können sich nicht selber vermehren, was sie von Viren und Würmern unterscheidet. Die meisten haben einen interessanten Namen (SEX.EXE oder STARTME.EXE), der den Anwender zur Ausführung des Trojaners verleiten soll. Unmittelbar nach der Ausführung werden diese dann aktiv und formatieren z.B. die Festplatte. Eine spezielle Art eines Trojaners ist ein Dropper, der Viren 'droppt', d.h. in das Computersystem einpflanzt.

Zombie

Ein Zombie-PC ist ein Rechner, welcher mit Malwareprogrammen infiziert ist und es den Hackern erlaubt, Rechner per Fernsteuerung für ihre kriminellen Zwecke zu missbrauchen. Der betroffene PC startet auf Befehl beispielsweise Denial-of-Service- (DoS) Attacken oder versendet Spam und Phishing Emails.

17. Info und Service

In diesem Kapitel erhalten Sie Informationen, auf welchen Wegen Sie mit uns in Kontakt treten können.

- siehe Kapitel Kontaktadresse
- siehe Kapitel Technischer Support
- siehe Kapitel Verdächtige Datei
- siehe Kapitel Fehlalarm melden
- siehe Kapitel Ihr Feedback für mehr Sicherheit

17.1 Kontaktadresse

Gerne helfen wir Ihnen weiter, wenn Sie Fragen und Anregungen zur Avira Produktwelt haben. Unsere Kontaktadressen finden Sie im Control Center unter **Hilfe > Über Avira Antivirus Suite**.

17.2 Technischer Support

Der Avira Support steht Ihnen zuverlässig zur Seite, wenn es gilt, Ihre Fragen zu beantworten oder ein technisches Problem zu lösen.

Auf unserer Webseite erhalten Sie alle nötigen Informationen zu unserem umfangreichen Support-Service:

http://www.avira.com/de/support

Damit wir Ihnen schnell und zuverlässig helfen können, sollten Sie die folgenden Informationen bereithalten:

- **Lizenzdaten**. Diese finden Sie auf der Programmoberfläche unter dem Menüpunkt **Hilfe > Über Avira Antivirus Suite > Lizenzinformationen**. Siehe Lizenzinformationen.
- **Versionsinformationen**. Diese finden Sie auf der Programmoberfläche unter dem Menüpunkt **Hilfe > Über Avira Antivirus Suite > Versionsinformationen**. Siehe Versionsinformationen.
- **Betriebssystemversion** und eventuell installierte Service-Packs.
- **Installierte Software-Pakete**, z.B. Antivirensoftware anderer Hersteller.
- **Genaue Meldungen** des Programms oder der Reportdatei.

17.3 Verdächtige Dateien

Sie können verdächtige Dateien oder Viren, die gegebenenfalls von unseren Produkten noch nicht erkannt bzw. entfernt werden können, an uns senden. Dafür stellen wir Ihnen mehrere Möglichkeiten zur Verfügung.

- Wählen Sie die Datei im Quarantänemanager des Control Centers aus und wählen Sie über das Kontextmenü oder die entsprechende Schaltfläche den Punkt **Datei senden**.
- Senden Sie die gewünschte Datei komprimiert (WinZIP, PKZip, Arj usw.) im Anhang einer Email an folgende Adresse:
  virus-premium@avira.de
  Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Passwort versehen (bitte nicht vergessen, uns das Passwort mitzuteilen).
- Alternativ haben Sie die Möglichkeit, die verdächtige Datei über unsere Webseite an uns zu senden: http://www.avira.de/sample-upload

17.4 Fehlalarm melden

Sind Sie der Meinung, dass Avira Antivirus Suite einen Fund in einer Datei meldet, die jedoch mit hoher Wahrscheinlichkeit "sauber" ist, so senden Sie diese Datei, gepackt (WinZIP, PKZIP, Arj, etc.) im Anhang einer Email, an folgende Adresse:

virus-premium@avira.de

Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).

17.5 Ihr Feedback für mehr Sicherheit

Bei Avira steht die Sicherheit unserer Kunden an erster Stelle. Aus diesem Grund beschäftigen wir nicht nur ein eigenes Expertenteam, welches jede einzelne Avira Lösung und jedes einzelne Update vor der Veröffentlichung aufwendigen Qualitäts- und Sicherheitstests unterzieht. Für uns gehört auch dazu, Hinweise auf eventuell auftretende, sicherheitsrelevante Schwachstellen ernst zu nehmen und mit diesen offen umzugehen.

Wenn Sie glauben, eine sicherheitsrelevante Schwachstelle in einem unserer Produkte gefunden zu haben, senden Sie bitte eine Email an folgende Adresse:

vulnerabilities-premium@avira.de



Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira Operations GmbH & Co. KG nicht gestattet.

Hier verwendete Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

Ausgabe Q4/2013

Avira | Kaplaneiweg 1 | 88069 Tettnang | Germany | Telefon: +49 7542-500 0
www.avira.de